Smartfuture
Certifications | Training | Technology solutions

Formation

Se préparer à la Certification CISSP

Formation présentielle et en ligne à la demande. Maîtrisez les 8 domaines du référentiel CISSP (ISC)² et préparez-vous efficacement à l'examen de certification international en cybersécurité.

Préparation à l'examen | Présentiel & distanciel | Animée par des experts cybersécurité

Durée 5 jours (35–40 h)	**Format** Présentiel / En ligne
Examen CISSP (ISC)²	**Niveau** Avancé / Expert

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

OBJECTIFS PÉDAGOGIQUES

- Comprendre en profondeur les 8 domaines du Common Body of Knowledge (CBK) CISSP.
- Identifier, analyser et traiter les risques de sécurité de l'information dans l'entreprise.
- Concevoir et mettre en œuvre une architecture de sécurité cohérente et alignée au business.
- Maîtriser les bonnes pratiques d'exploitation, de tests, d'architecture et de développement sécurisé.

PUBLIC CIBLE

- Responsables PCA / Continuité d'activité, Risk managers.
- RSSI, DSI, chefs de projet et architectes systèmes / réseaux.
- Consultants en sécurité, auditeurs, experts en conformité.
- Professionnels IT expérimentés souhaitant valider leur expertise par un titre international.

PRÉREQUIS

- Connaissances solides en systèmes, réseaux, sécurité et gouvernance IT.
- Expérience professionnelle recommandée : 3 à 5 ans dans un ou plusieurs domaines de la sécurité.
- Niveau d'anglais de lecture suffisant pour l'examen officiel (questions en anglais).

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Sécurité et gestion des risques

Fondamentaux de la sécurité de l'information

- Principes de confidentialité, intégrité, disponibilité (CIA) et autres concepts fondamentaux.
- Gouvernance, stratégie de sécurité et alignement sur les objectifs métiers.
- Politiques, standards, procédures, lignes directrices : structure et mise en œuvre.

Gestion des risques, conformité et éthique

- Cadres de gestion des risques (ISO 27005, NIST, etc.).
- Identification, analyse, traitement et suivi des risques.
- Notions de conformité : lois, réglementations, RGPD, contrats et obligations légales.
- Études d'impact (BIA), continuité d'activité (BCP) et reprise après sinistre (DRP).
- Éthique professionnelle, code de déontologie (ISC)², gestion des conflits d'intérêt.

Sécurité des actifs

Classification et gestion des informations et des actifs

- Inventaire, propriété et responsabilité des actifs d'information.
- Classification des données (publique, interne, confidentielle, secrète, etc.).
- Gestion du cycle de vie de l'information : création, stockage, utilisation, archivage, destruction.

Protection des données et de la vie privée

- Techniques de protection des données (masquage, chiffrement, anonymisation, tokenisation).
- Gestion des supports (papier, disques, sauvegardes, médias amovibles).
- Protection de la vie privée et données personnelles, exigences réglementaires.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Architecture et ingénierie de la sécurité

Concepts de base d'architecture de sécurité

- Modèles de sécurité (Bell-LaPadula, Biba, Clark-Wilson, etc.).
- Conception sécurisée des systèmes : confiance, domaines de sécurité, zones, cloisonnement.
- Sécurité des systèmes d'exploitation, virtualisation, containers et environnements cloud.

Cryptographie et technologies de sécurité

- Concepts clés : clés symétriques, asymétriques, hachage, signatures numériques, PKI.
- Gestion des clés, certificats, autorités de certification.
- Sécurisation du matériel : HSM, TPM, cartes à puce.

Sécurité des architectures modernes

- Sécurité des architectures distribuées, microservices et API.
- IoT, systèmes industriels (SCADA/ICS), environnements embarqués.

Sécurité des communications et des réseaux

Concepts et architectures réseaux

- Modèles OSI et TCP/IP, topologies, composants réseaux.
- Segmentation, VLAN, routage, commutation, DMZ, zones de sécurité.

Sécurisation des communications

- Protocoles sécurisés (TLS, IPsec, SSH, etc.).
- VPN, accès distants, réseaux privés virtuels pour les utilisateurs nomades.
- Sécurité Wi-Fi, VoIP, communications temps réel.
- Equipements de sécurité : pare-feu, IDS/IPS, proxies, WAF.

Gestion des identités et des accès (IAM)

Gestion des identités

- Cycle de vie des identités : création, modification, révocation.
- Modèles d'identités : comptes utilisateurs, comptes privilégiés, comptes de service.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Contrôle d'accès et authentification

- Modèles de contrôle d'accès : RBAC, ABAC, DAC, MAC.
- Mécanismes d'authentification : mots de passe, MFA, biométrie, tokens.
- Autorisations, sessions, journalisation des accès, principe du moindre privilège.

Fédération et SSO

- SSO, fédération d'identités, SAML, OAuth, OpenID Connect.
- Gestion des accès aux ressources cloud et hybrides.

Évaluation et tests de sécurité

Stratégie et planification des tests

- Objectifs et types de tests de sécurité (tests techniques et organisationnels).
- Plan de test, périmètre, critères d'acceptation, reporting.

Techniques d'évaluation

- Analyses de vulnérabilités, scans automatisés, revues de configuration.
- Tests d'intrusion (pentests), tests de résistance, red teaming (concepts).
- Audits de sécurité, audits de conformité, revues de code.

Exploitation des résultats

- Interprétation des rapports, priorisation des corrections.
- Gestion des plans d'actions correctives, re-tests et suivi.

Opérations de sécurité

Organisation et processus opérationnels

- Fonction SOC, surveillance et supervision de la sécurité.
- Gestion des journaux, corrélation des événements, SIEM.
- Gestion des changements, des incidents et des problèmes.

Gestion des incidents de sécurité

- Cycle de gestion d'incident : préparation, détection, analyse, confinement, éradication, reprise.
- Forensique numérique : principes, collecte et préservation de la preuve.

Continuité, sauvegarde et résilience

- Stratégies de sauvegarde et de restauration, RTO, RPO.
- Sites de secours, plans BCP/DRP, exercices et tests.

Sécurité du développement logiciel

Intégration de la sécurité dans le cycle de développement

- SDLC classique, Agile, DevOps / DevSecOps.
- Exigences de sécurité, revues de conception et de code.

Sécurité applicative

- Principales vulnérabilités applicatives (injection, XSS, CSRF, etc.).
- Mécanismes de protection côté serveur et côté client.
- Tests de sécurité applicative, analyse de code statique/dynamique.

Atelier de préparation à l'examen CISSP

Méthodologie et stratégie d'examen

- Format de l'examen CISSP, nombre de questions, barème, durée.
- Méthode de lecture et d'analyse des questions, élimination des distracteurs.
- Gestion du temps, de la fatigue et du stress le jour J.

Exercices et revue finale

- Séries de questions type examen sur les 8 domaines.
- Correction collective et justification détaillée des réponses.
- Plan d'action personnalisé pour finaliser sa préparation après la formation.