Présentiel/distanciel | Cours Officiel | Formation certifiante

CISSP : Certification en Sécurité des Systèmes d'Information (Certified Information Systems Security Professional)

Objectifs pédagogiques

- Analyser les enjeux de sécurité des systèmes d'information à l'échelle d'une organisation
- Maîtriser les 8 domaines du Common Body of Knowledge (CBK) CISSP
- Évaluer les risques et définir des politiques de sécurité adaptées
- Concevoir une architecture de sécurité cohérente et robuste
- Mettre en oeuvre des mécanismes de protection des systèmes, réseaux et applications
- Contrôler et auditer la posture de sécurité d'un système d'information
- Structurer une démarche de gouvernance et d'amélioration continue de la sécurité

Prérequis

- Expérience professionnelle en informatique (réseaux, systèmes, développement ou sécurité)
- Connaissances fondamentales en sécurité des systèmes d'information
- Compréhension des architectures IT et des environnements réseaux

Afin d'obtenir la certification CISSP, il faudra justifier de 5 ans d'expérience professionnelle dans au moins 2 des 8 domaines du CBK®. Un candidat qui n'a pas l'expérience requise pour obtenir la certification CISSP peut passer l'examen et obtenir le titre de CISSP Associate. Il aura alors jusqu'à 6 ans pour acquérir les 5 années d'expérience requises.

Public concerné

Professionnels expérimentés de l'informatique et de la cybersécurité souhaitant valider et structurer leur expertise :

- Ingénieurs systèmes et réseaux
- Consultants en cybersécurité
- Architectes sécurité
- Responsables sécurité (RSSI) ou futurs RSSI
- Auditeurs IT et sécurité

Cette formation permet d'acquérir une vision globale et structurée de la sécurité des systèmes d'information, directement exploitable dans des fonctions à forte responsabilité.

Certification

Cette formation prépare au passage de l'examen de la certification Certified Information Systems Security Professional (CISSP), dont le voucher est compris dans le coût de la formation en inter-entreprises.

Conditions de passage d'examen :

Examen en langue anglaise

Durée : 3 heures

Nombre de questions : entre 100 et 150 questions (le nombre de questions est variable car il dépend des questions et réponses précédentes)

Score requis : 700/1000

Examen en langue française

Durée : 6 heures

Nombre de questions : 250

Type de questions : choix multiples et questions avancées innovantes

Score requis : 700/1000

Programme détaillé

Gouvernance de la sécurité et gestion des risques (CBK 1) 5h00

- Principes fondamentaux : confidentialité, intégrité, disponibilité
- Gouvernance de la sécurité et alignement stratégique
- Gestion des risques : identification, analyse et traitement
- Conformité réglementaire et exigences légales
- Politiques, normes et procédures de sécurité
- Continuité d'activité et gestion de crise

Sécurité des actifs (CBK 2) 3h30

- Classification et gestion des actifs informationnels
- Protection des données sensibles
- Gestion du cycle de vie de l'information
- Exigences de confidentialité et de protection des données

Architecture et ingénierie de sécurité (CBK 3) 5h30

- Modèles de sécurité et architectures sécurisées
- Cryptographie et gestion des clés
- Sécurité des systèmes et des infrastructures
- Sécurité matérielle et physique
- Concepts de confiance et de sécurité des composants

Sécurité des communications et des réseaux (CBK 4) 4h30

- Protocoles réseau sécurisés
- Segmentation réseau et défense en profondeur
- Sécurisation des communications
- Protection contre les attaques réseau

Gestion des identités et des accès (CBK 5) 3h30

- Concepts IAM (Identity and Access Management)
- Authentification, autorisation et traçabilité
- Modèles de contrôle d'accès (RBAC, ABAC...)
- Gestion des identités et des privilèges

Documentation

Support de cours officiel en anglais

Évaluation et audit de la sécurité (CBK 6) 4h00

- Méthodologies d'audit et de test de sécurité
- Indicateurs de performance sécurité
- Tests d'intrusion et analyses de vulnérabilités
- Contrôles et conformité

Opérations de sécurité (CBK 7) 5h00

- Supervision et gestion des incidents (SOC)
- Gestion des vulnérabilités
- Réponse aux incidents et forensic
- Continuité et reprise d'activité
- Gestion des journaux et monitoring

Sécurité du développement logiciel (CBK 8) 4h00

- Intégration de la sécurité dans le cycle de développement (SSDLC)
- Vulnérabilités applicatives (OWASP)
- Tests de sécurité applicative
- Bonnes pratiques de développement sécurisé

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

Le cours est assuré par un formateur certifié CISSP et professionnel aguerri de la Sécurité, pour apporter aux participants une vision pragmatique terrain » de chacune des thématiques abordées.
A la fin de chaque module, les participants s'entraînent à répondre à un ensemble de questions portant sur le thème exposé et un examen à blanc, similaire à l'examen officiel, est inclus dans la formation.

Accessibilité de la formation