

Formation Sécurité Préparation à la certification CISSP

Présentation

La certification CISSP (Certified Information Systems Security Professional) est l'une des certifications en cybersécurité les plus reconnues au niveau international, délivrée par l'International Information System Security Certification Consortium (ISC)².

L'objectif de cette formation est de vous préparer de manière complète et approfondie à réussir l'examen CISSP et à devenir un professionnel compétent en cybersécurité, capable de relever les défis de sécurité de l'information dans un environnement en constante évolution.

L'achat du voucher pour passer la certification est en option.

Durée : 35,00 heures (5 jours)

Tarif INTRA : Nous consulter

Objectifs de la formation

- Comprendre les concepts fondamentaux de la cybersécurité
- Connaître les huit domaines de connaissances de la CISSP
- Appliquer les meilleures pratiques en cybersécurité
- Respecter le code d'éthique de l'ISC²
- Se préparer à l'examen CISSP

Prérequis

Connaissance de base en cybersécurité : Il est préférable d'avoir des connaissances de base en cybersécurité, y compris les concepts de sécurité de l'information, les principes de gestion des risques, les mécanismes de sécurité etc...

Public

Auditeurs confirmés ou informaticiens (DSI, RSSI, Managers, Ingénieurs, Experts Consultants) qui souhaitent se préparer à la certification à l'examen CISSP (Certified Information System Security Professional) délivrée par l'ISC².

Programme de la formation



1/ Introduction à la CISSP et planification

- Familiarisez-vous avec le processus d'inscription à la certification CISSP et les exigences d'expérience professionnelle.
- Planifiez votre programme d'étude en accordant une attention particulière aux domaines où vous avez moins d'expérience.

2/ Sécurité et gestion des risques

- Comprendre les concepts de gestion des risques en cybersécurité.
- Apprendre les principes de la gestion des risques, y compris l'identification, l'évaluation et la gestion des risques de sécurité.

3/ Sécurité des actifs

- Étudier les principes de la classification des actifs et de la gestion des actifs de l'organisation.
- Apprendre à protéger les actifs informatiques, y compris les données sensibles et les propriétés intellectuelles.

4/ Architecture et ingénierie de la sécurité

- Comprendre les principes de conception et d'architecture sécurisées pour les systèmes, les réseaux et les applications.
- Étudier les mécanismes de sécurité tels que la cryptographie, les pare-feu, les IDS/IPS, etc.

5/ Communication et gestion des identités

- Apprendre les concepts de communication sécurisée, y compris les protocoles cryptographiques et la sécurité des réseaux sans fil.
- Étudier la gestion des identités, l'authentification et les techniques de contrôle d'accès.

6/ Gestion des accès et de l'authentification

- Approfondir les concepts de contrôle d'accès, d'authentification multifactorielle et d'autorisation.
- Comprendre les meilleures pratiques pour gérer les droits d'accès des utilisateurs.

7/ Sécurité des opérations

- Apprendre à gérer les incidents de sécurité, les mesures de réponse aux incidents et la reprise après sinistre.
- Étudier les principes de la surveillance et de la gestion des journaux.

8/ Évaluation et tests de sécurité

- Comprendre les concepts d'évaluation de la sécurité, y compris les tests de pénétration et les audits de sécurité.
- Apprendre à évaluer les vulnérabilités et les risques liés à la sécurité.

9/ Gestion des logiciels de sécurité

- Étudier la gestion du cycle de vie du développement sécurisé des logiciels.
- Comprendre les meilleures pratiques pour assurer la sécurité des applications et des logiciels utilisés par l'organisation.

Organisation

Formateur

Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes.

Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétence.

Moyens pédagogiques et techniques

- Alternance d'apports théoriques et de mises en pratique contextualisées.
- Progression pédagogique structurée, de la compréhension à la mise en œuvre opérationnelle.
- Pédagogie immersive favorisant une mise en application immédiate des compétences.
- Formation interactive et participative s'appuyant sur des ateliers pratiques, études de cas et échanges collectifs (+ 60 % du temps de formation.)
- Séquences pédagogiques rythmées et évaluations formatives régulières pour renforcer l'ancrage des apprentissages.
- Supports de cours, ressources documentaires et références mis à disposition par le formateur

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation *(évaluation en ligne dans l'extranet apprenant)*

- Recueil des besoins et des attentes des participants.
- Auto-positionnement permettant d'évaluer le niveau initial des apprenants.

Tout au long de la formation

- Évaluations continues réalisées par le formateur à travers des questions orales, exercices, QCM, études de cas et mises en situation pratiques.

À l'issue de la formation *(évaluations en ligne dans l'extranet apprenant)*

- Auto-positionnement afin de mesurer l'acquisition des compétences visées.
- Validation de l'acquisition des compétences par le formateur
- Questionnaire de satisfaction « à chaud » à l'issue de la formation
- Questionnaire de satisfaction "à froid", 45 jours après la formation afin d'évaluer l'ancrage des acquis et leur mise en application en situation professionnelle.

Accessibilité

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.