CISSP-ISSAP® : spécialiste en architecture de la sécurité des SI

Date et durée
Code formation : CIS02FR Durée : 5 jours Nombre d'heures : 35 heures
Formation avec préparation à la certification
CISSP® : Certified Information Systems Security Professional
Description

Dans le **domaine de la sécurité de l'information**, si vous occupez un poste à responsabilités, le CISSP-ISSAP est le meilleur programme de spécialisation à suivre. Que vous souhaitiez faire progresser votre carrière, affiner vos compétences ou obtenir un titre professionnel de haut niveau, la **formation CISSP-ISSAP concentration** est un choix judicieux. Elle démontre la parfaite compréhension que vous avez acquise dans la mise en œuvre des architectures de sécurité des SI.
Cette formation, **destinée aux architectes et aux analystes** responsables de la sécurité des SI, repose sur le CISSP et le Common Body of Knowledge (ISC² CBK®). Elle permet de maitriser les nombreux domaines couverts par ce corpus de connaissances et couvre également les questions liées aux menaces, aux technologies, aux règlementations, ainsi qu'aux normes et aux meilleures pratiques. Dans chaque cours CISSP-ISSAP, **les 6 domaines suivants seront couverts** :

- Domaine 1 : l'architecte pour la gouvernance, la conformité et la gestion des risques ;
- Domaine 2 : la modélisation de l'architecture de sécurité ;
- Domaine 3 : l'architecture de sécurité de l'infrastructure ;
- Domaine 4 : l'architecture de gestion des identités et des accès ;
- Domaine 5 : l'architecte de la sécurité des applications ;
- Domaine 6 : l'architecture des opérations de sécurité.

À l'issue de cette formation de 5 jours, vous serez en outre préparé pour **passer l'examen (ISC)² CISSP-ISSAP**. Cet examen que vous pourrez passer dans notre centre Pearson VUE vous permettra d'obtenir le titre de **Certified Information Systems Security Architecture Professional** (*pour plus d'informations, consultez l'onglet Certification*).

En partenariat avec ISC2®, Oo2 vous garantit un contenu de formation officiel et actualisé. Les cours sont dispensés par un formateur expert en sécurité informatique et agréé pour dispenser cette formation CISSP-ISSAP.

Objectifs

A l'issue de la **formation CISSP-ISSAP**, vous serez capable de valider les objectifs de compétences suivants :

- définir les exigences légales, organisationnelles et industrielles pour la conception d'une architecture de sécurité ;
- maitriser les étapes du management des risques ;
- identifier la stratégie d'architecture de sécurité à mettre en place ;
- vérifier et valider la conception d'une l'architecture ;
- établir les exigences de sécurité d'une l'infrastructure ;
- concevoir une architecture de défense en profondeur ;
- sécuriser les services partagés ;
- mettre en place des contrôles techniques de sécurité ;
- concevoir et intégrer un système de surveillance pour une infrastructure ;
- concevoir des solutions cryptographiques pour l'infrastructure ;
- concevoir une infrastructure de réseau et de communication sécurisée ;
- évaluer les exigences de sécurité physique et environnementale ;
- concevoir la gestion et le cycle de vie de l'identité et du contrôle d'accès ainsi que des solutions d'identité et d'accès ;
- intégrer le cycle de vie du développement logiciel (SDLC) à l'architecture de sécurité des applications ;
- déterminer les besoins et la stratégie en matière de sécurité des applications ;
- identifier les contrôles proactifs communs pour les applications et les besoins liés aux opérations de sécurité ;
- concevoir la surveillance de la sécurité de l'information ;
- concevoir des solutions de continuité des activités et de résilience ;
- valider l'architecture du plan de continuité des activités (PCA) et du plan de reprise après sinistre (PRA) ;
- concevoir la gestion de la réponse aux incidents de cybersécurité ;
- être bien préparé pour le passage l'examen officiel CISSP-ISSAP.

Points forts

Un formateur agréé (ISC)², des supports de cours officiels, une préparation complète pour le passage de la certification CISSP-ISSAP, des conseils et des quiz d'évaluations pour chacun des 6 domaines abordés.

Certification

Cette formation qui vous prépare à l'examen CISSP-ISSAP, vous permettra d'obtenir le titre de **Certified Information Systems Security Architecture Professional** délivrée par notre partenaire *(ISC)² ®. Il convient si vous êtes un professionnel de la sécurité des systèmes d'information et que vous êtes titulaire de la certification*

CISSP - Certified Information Systems Security Professional.
Le CISSP-ISSAP démontre que vous avez acquis une **expertise dans le développement, la conception et l'analyse de solutions de sécurité des SI**. Il atteste également de votre capacité à fournir des recommandations fondées sur les risques pour atteindre les objectifs opérationnels de l'entreprise.

Information sur l'examen CISSP-ISSAP :

- Durée : 3 heures max
- Langue de l'examen : anglais
- Nombre de questions :125
- Format des questions : choix multiple
- Note de passage : 700 sur 1000 points

A savoir : *après avoir passé l'examen CISSP-ISSAP et obtenu la certification, vous devez renouveler votre certification tous les 3 ans. Pour cela, vous devez obtenir 20 crédits de formation professionnelle continue (FPC) chaque année. Vous pouvez utiliser ces 20 crédits dans le cadre de votre exigence de formation continue CISSP, à condition que les crédits soient spécifiques à l'architecture de sécurité.*
Pour passer l'examen de certification CISSP-ISSAP, vous pouvez vous rendre dans notre centre Pearson VUE Oo2 Formations.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CISSP-ISSAP** nécessite les prérequis suivants :

- détenir le titre professionnel CISSP à jour et justifier de 2 ans d'expérience professionnelle cumulée dans un ou plusieurs des 6 domaines du corpus de connaissances (ISC)² CBK.

Pour obtenir la certification CISSP, vous pouvez suivre notre formation :

Les formations ci-dessous sont recommandées.

CISSP® : devenir expert en sécurité des SI

Public

Cette formation s'adresse aux publics suivants :

- les responsables de la sécurité des SI, les architectes ou toute autre personne intervenant dans la politique de sécurité des systèmes d'information.

Cette formation s'adresse aux profils suivants

Architecte informatique / SI
Administrateur système
Ingénieur système
Directeur des Systèmes d'Information (DSI)

Programme

Domaine 1 : gouvernance, conformité et gestion des risques pour les architectures des SI

- Les normes et réglementations applicables en matière de sécurité de l'information.
- Les obligations des tiers et les obligations contractuelles (chaîne d'approvisionnement, externalisation, sous-traitance, etc.).
- Les normes et directives applicables en matière de protection des données (RGPD).
- La conception pour l'auditabilité des SI (exigences réglementaires, législatives, médicolégales, ségrégation, systèmes d'assurance élevée, etc.).
- La coordination avec des acteurs externes (services de police, relations publiques, expert indépendant, etc.).
- L'identification et la classification des risques.
- La mise en place de recommandations pour le traitement des risques (atténuation, transfert, acceptation, évitement, etc.).
- La surveillance et le rapport des risques.

Domaine 2 : modélisation de l'architecture de sécurité

- Les types et le champ d'application (entreprise, réseau, architecture orientée services (SOA), cloud, IoT), systèmes de contrôle industriel (ICS) et SCADA (Supervisory Control and Data Acquisition).
- Les frameworks (Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF).
- Les architectures et les plans de référence.
- La configuration de la sécurité (les bases, les benchmarks, les profils, etc.).
- La configuration du réseau (physique, logique, haute disponibilité, segmentation et zones).
- La validation des résultats de la modélisation des menaces vecteurs de menace, conséquences et probabilités).
- L'identification des failles et des solutions alternatives.
- La vérification et la validation indépendantes (exercices sur table, modélisation et simulation, examen manuel des fonctions).

Domaine 3 : architecture de sécurité de l'infrastructure

- Les prérequis pour un système sur site, dans le cloud et hybride.
- L'Internet des objets (IoT) et la confiance zéro.
- Le management des réseaux.
- La sécurité des systèmes de contrôle industriel (ICS).
- La sécurité des réseaux.
- La sécurité des systèmes d'exploitation (OS).
- La sécurité des bases de données.
- La sécurité des conteneurs.
- La sécurité des charges de travail dans le cloud.
- La sécurité des firmwares.
- Les questions de sensibilisation à la sécurité des utilisateurs.
- Les sécurisation des services partagés (Wi-Fi, e-mail, voix sur IP, communication unifiée, DNS et NTP).
- La protection des limites de la conception (firewalls, VPN, Air gap, périmètres définis par logiciel, wireless, cloud-native).
- La gestion des dispositifs sécurisés (Bring Your Own Device (BYOD), mobile, serveur, endpoint, cloud instance et stockage).
- La visibilité du réseau (placement des capteurs, réconciliation temporelle, étendue du contrôle et compatibilité des enregistrements).
- Les solutions de collecte active et passive (span port, port mirroring, tap, inline et logs de flux).

- Les analyses de sécurité (collecte de logs, machine learning, User Behavior Analytics (UBA), Security Information and Event Management (SIEM).
- Les considérations et les contraintes de la conception cryptographique.
- La mise en œuvre cryptographique.
- La planification du cycle de vie de la gestion des clés (génération, stockage, distribution, etc.).
- La conception d'une infrastructure de réseau et de communication sécurisée (VPN, IPsec, et TLS).
- L'adaptation des exigences de sécurité physique aux besoins de l'entreprise (protection du périmètre, zonage interne, extinction des incendies, etc.).
- La validation des contrôles de sécurité physique et de l'environnement.

Domaine 4 : architecture de gestion des identités et des accès

- L'identification et la vérification des identités.
- L'attribution des identifiants aux utilisateurs, services, processus et aux périphériques.
- Le provisionnement et le dé-provisionnement des identités.
- Les relations de confiance fédérée et autonome.
- Les méthodes d'authentification (authentification multifactorielle (MFA), basée sur les risques, basée sur l'emplacement, basée sur les connaissances, basée sur les objets, basée sur les caractéristiques).
- Les protocoles et technologies d'authentification (SAML, RADIUS, Kerberos, etc.).
- Les concepts et les principes du contrôle d'accès.
- Les type de configuration du contrôle d'accès (physique, logique, et administratif).
- Le processus d'autorisation et le flux de travail (gouvernance, émission, révision périodique et révocation).
- Les rôles, les droits et les responsabilités liés au contrôle d'accès aux systèmes, aux applications et aux données.
- La gestion des comptes privilégiés et leurs autorisations.
- Les protocoles et technologies de contrôle d'accès (XACML et LDAP).
- Les technologies de gestion des autorisations (mots de passe, certificats, et cartes à puce).
- L'architecture centralisée et décentralisée pour la gestion des identités et des accès.
- L'implémentation de la gestion des accès privilégiés (PAM).
- La comptabilité pour la journalisation, le suivi et l'audit.

Domaine 5 : sécurité des applications pour l'architecture

- L'évaluation de la méthode de révision du code (dynamique, manuelle, statique, etc.).
- L'évaluation des besoins liés à la protection des applications (pare-feu d'application Web, anti-malware, API sécurisée et SAML sécurisé.
- Les exigences de cryptage au repos, en transit et en cours d'utilisation).
- Les exigences liées à la sécurité des communications entre les applications et les bases de données ou d'autres points de terminaison doivent être évaluées.
- L'utilisation d'un dépôt de code sécurisé.
- L'analyse de la sécurité des applications.
- Le choix d'une solution cryptographique pour les applications (interface de programmation d'application cryptographique, générateur de nombres pseudo-aléatoires et gestion des clés).
- L'analyse de la possibilité d'appliquer des contrôles de sécurité aux composants du système.
- L'identification des contrôles proactifs communs pour les applications avec Open Web Application Security Project (OWASP).

Domaine 6 : architecture des opérations de sécurité

- Les exigences des opérations de sécurité (légales, conformité, organisationnelles et commerciales).
- La détection et l'analyse.
- La surveillance proactive et automatisée de la sécurité et la remédiation (gestion des vulnérabilités, audit de conformité et tests de pénétration).
- L'intégration de l'analyse de l'impact sur les affaires (BIA).

- Le choix d'une stratégie de récupération et de viabilité.
- Les solutions de continuité et de disponibilité (sauvegarde à froid, à chaud et dans le cloud).
- Les exigences des accords de traitement (fournisseur, réciproque, mutuel, cloud et virtualisation).
- Les objectifs de temps de récupération (RTO) et de points de récupération (RPO).
- La mise en place d'un système de communication d'urgence sécurisé pour les opérations.
- La validation de l'architecture du plan de continuité des activités et du plan de reprise après sinistre.
- La préparation (plan de communication, plan de réponse aux incidents et formation du personnel).
- L'identification.
- Le confinement.
- L'éradication.
- La récupération.
- L'analyse des expériences acquises.

Contenu de formation proposé en partenariat avec (ISC)² ®
CISSP® et CISSP-ISSAP® sont des marques déposées de l'International Information Systems Security Certification.