Préparation à la Certification CISSP

★★★★★

SII-422 **5 Jours (35 Heures)**

Description

La certification CISSP® (Certified Information Systems Security Professional) est une certification mondiale, indépendante et reconnue, qui évalue les compétences en sécurité informatique sur trois axes : connaissances techniques, analyse des risques et audit des systèmes. Elle va au-delà de la maîtrise des technologies en prouvant la capacité à les intégrer pour répondre aux besoins de sécurité des organisations. Cette formation prépare à la certification CISSP.

À qui s'adresse cette formation ?

Pour qui

RSSI

DSI

Consultants

Auditeurs

Administrateurs Système et réseaux

Prérequis

Notions fondamentales sur :

- les réseaux
- les systèmes d'exploitation
- la sécurité de l'information

Les objectifs de la formation

- Acquérir une connaissance des thèmes, domaines et sections du Common Body of Knowledge (CBK®)
- Maîtriser les principes de base de la sécurité des systèmes d'information
- Se préparer à l'examen de certification CISSP

Programme de la formation

Protection des données et gestion des risques

- Les notions de confidentialité, d'intégrité et de disponibilité
- Les principes de la gouvernance en matière de sécurité
- La conformité
- Les interrogations juridiques et réglementaires relatives à la sécurité de l'information dans une perspective mondiale.
- La déontologie professionnelle
- Les normes de sécurité, les standards, les procédures et les directives.
- Les exigences en matière de continuité des opérations Les politiques de sécurité du personnel
- Les notions de gestion des risques
- Le schéma de menace
- Les enjeux de sécurité sont pris en compte dans la stratégie d'achat.
- La formation, l'éducation et la sensibilisation à la sécurité de l'information.

La protection des actifs

- Catégorisation de l'information et assistance liée aux actifs.
- La préservation de la propriété
- Préserver la confidentialité
- Veiller à la conservation adéquate
- Les mesures de protection des données
- Les exigences de traitement

Ingénierie dédiée à la sécurité

- Les principes de conception sécurisée et les processus d'ingénierie
- Assimiler les principes de base des modèles de sécurité.
- Les actions et réactions
- Les options de sécurité fournies par les systèmes d'information.
- Les failles de sécurité liées aux architectures, aux conceptions et aux solutions
- Examiner et minimiser les faiblesses de sécurité des systèmes web, mobiles et intégrés.
- La cryptographie
- Les principes de sécurité concernant le site et la conception de l'installation.
- La protection physique

Protection des réseaux et des télécommunications

- Les principes de sécurité incorporés dans l'architecture réseau.
- Protéger les éléments du réseau.
- Créer et mettre en place des voies de communication sécurisées.
- Éviter ou réduire les attaques sur le réseau

La gestion des accès et des identités

- Accès physique et logique contrôlé aux actifs
- S'occuper de l'identification et de l'authentification des individus et des appareils.
- Service d'identité en tant que service
- Les services d'identification tiers
- Mécanismes d'autorisation Attaques sur le contrôle d'accès
- Le cycle de vie des identités et la gestion du provisionnement des accès

Évaluation de la sécurité et réalisation de tests

- Les approches d'évaluation et de test en matière de sécurité
- Essais de vérification de la sécurité
- Les informations relatives aux processus de sécurité
- Les conclusions des tests
- Les contrôles internes ou par des tiers

Plan de continuité des activités et stratégie de récupération

- Les recherches
- Les critères des différentes sortes d'examens
- L'activité de suivi et d'enregistrement des activités La mise à disposition des ressources
- Les principes de base de la sécurité des opérations
- Les méthodes de sauvegarde des ressources
- La gestion des incidents
- Mettre en œuvre et assurer le maintien de mesures de sécurité préventives.
- Gestion des correctifs et des failles de sécurité
- Les procédures de gestion du changement
- Les tactiques de rétablissement
- Les stratégies de continuité d'activité après un sinistre
- Les stratégies de reprise après sinistre
- Le Plan de Continuité d'Activités
- La gestion de la sécurité physique
- Les enjeux de sécurité du personnel

La sécurité dans le développement de logiciels

- La sécurité au sein du cycle de vie du développement logiciel.
- Les dispositifs de sécurité dans les contextes de développement
- L'efficacité de la sécurité logicielle
- Évaluer l'effet de la sécurité d'un logiciel acheté