Professionnel Certifié en Sécurité des Systèmes d'Information (CISSP)

Durée: 5 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Consultant en sécurité
- Analyste de sécurité
- Manager de sécurité
- Ingénieur système de sécurité
- Directeur de la sécurité de l'information
- Directeur ou Gestionnaire informatique
- Auditeur de sécurité
- Directeur de la sécurité
- Architecte de sécurité
- Architecte réseau

Objectifs de la formation

- Comprendre les concepts de gestion des risques, les politiques de sécurité, et les cadres de conformité
- Protéger les informations et les actifs de l'organisation
- Concevoir et mettre en œuvre des solutions de sécurité robustes
- Assurer la sécurité des réseaux et des communications
- Gérer les identités et les accès pour garantir que seules les personnes autorisées ont accès aux ressources
- Évaluer et tester les systèmes de sécurité pour identifier les vulnérabilités
- Gérer les opérations de sécurité au quotidien
- Intégrer des pratiques de sécurité dans le cycle de vie du développement logiciel

Description sommaire

En participant à cette formation intensive de cinq jours axés sur les connaissances, vous serez préparé par un expert pour concevoir, mettre en œuvre et gérer des programmes de sécurité de l'information. Cette formation est conçue pour vous aider à vous préparer à l'examen CISSP.

Contenu du plan de cours

Module 1 : Sécurité et gestion des risques

- Comprendre et appliquer les concepts de confidentialité, d'intégrité et de disponibilité
- Appliquer les principes de gouvernance de la sécurité
- Conformité
- Comprendre les questions juridiques et réglementaires qui se rapportent à la sécurité de l'information dans un contexte mondial
- Élaborer et mettre en œuvre une politique de sécurité documentée, des normes, des procédures et des lignes directrices
- Comprendre les exigences de continuité des affaires
- Contribuer aux politiques de sécurité du personnel
- Comprendre et appliquer les concepts de gestion des risques
- Comprendre et appliquer la modélisation des menaces
- Intégration des facteurs de risque de sécurité dans la stratégie et la pratique d'acquisition
- Établir et gérer l'éducation, la formation et la sensibilisation à la sécurité

Module 2 : Sécurité des biens

- Classer les informations et soutenir les ressources
- Déterminer et maintenir la propriété
- Protéger la vie privée
- Assurer une rétention appropriée
- Déterminer les contrôles de sécurité des données
- Établir les exigences de manutention

Module 3 : Ingénierie de la sécurité

- Implémentation et gestion d'un cycle de vie d'ingénierie à l'aide des principes de conception de sécurité
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles et les contre-mesures en fonction des normes de sécurité des systèmes d'information
- Comprendre les capacités de sécurité des systèmes d'information
- Évaluer et atténuer les vulnérabilités des architectures de sécurité, des conceptions et des éléments de solution
- Évaluer et atténuer les vulnérabilités dans les systèmes Web
- Évaluer et atténuer les vulnérabilités dans les systèmes mobiles
- Évaluer et atténuer les vulnérabilités dans les dispositifs embarqués et les systèmes cyber-physiques
- Appliquer la cryptographie
- Appliquer des principes sécurisés à la conception du site et de l'installation
- Conception et implémentation de la sécurité des installations

Module 4 : Communications et sécurité réseau

- Appliquer des principes de conception sécurisés à l'architecture de réseau
- Sécurisation des composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou atténuer les attaques réseau

Module 5 : Gestion des identités et des accès

- Contrôler l'accès physique et logique aux ressources
- Gérer l'identification et l'authentification des personnes et des périphériques
- Intégrer l'identité en tant que service (IDaaS)
- Intégration des services d'identité tiers
-

Implémenter et gérer les mécanismes d'autorisation

- Prévention ou atténuation des attaques de contrôle d'accès
- Gérer le cycle de vie du provisionnement d'identité et d'accès

Module 6 : Évaluation et test de sécurité

- Concevoir et valider des stratégies d'évaluation et de test
- Effectuer des tests de contrôle de sécurité
- Collecte des données du processus de sécurité
- Mener ou faciliter les vérifications internes et externes

Module 7 : Opérations de sécurité

- Comprendre et soutenir les enquêtes
- Comprendre les exigences pour les types d'enquête
- Diriger les activités d'exploitation forestière et de surveillance
- Sécurisation du provisionnement des ressources via la gestion de la configuration
- Comprendre et appliquer les concepts fondamentaux des opérations de sécurité
- Employer des techniques de protection des ressources
- Intervention en cas d'incident
- Exploiter et maintenir les mesures préventives
- Implémentation et prise en charge du correctif et de la gestion des vulnérabilités
- Participer et comprendre les processus de gestion du changement
- Implémenter des stratégies de récupération
- Implémenter les processus de récupération après sinistre
- Test de catastrophe
- Participer à la planification de la continuité des activités
- Implémenter et gérer la sécurité physique
- Participer à la sécurité du personnel

Module 8 : Sécurité du développement logiciel

- Comprendre et appliquer la sécurité dans le cycle de vie du développement logiciel
- Appliquer les contrôles de sécurité dans l'environnement de développement
- Évaluer l'efficacité de la sécurité logicielle
- Évaluer la sécurité d'acquisition de logiciels

Approche et méthode pédagogique

Exposés structurés permettant de couvrir l’ensemble des domaines du CISSP et d’en comprendre les concepts clés. Présentation de cadres, normes et bonnes pratiques en sécurité de l’information afin de renforcer les connaissances théoriques. Études de cas et exemples concrets facilitant l’application des concepts dans des contextes professionnels réels. Exercices de révision et questions de type examen favorisant la préparation à la certification. Échanges et clarification avec le formateur expert pour approfondir la compréhension et répondre aux questions.

Prérequis

- Cinq ans d'expérience dans l'infrastructure informatique et la cybersécurité

Recommandations

Cette formation s’adresse à des professionnels expérimentés en cybersécurité ou en infrastructure TI souhaitant se préparer à la certification CISSP. Il est recommandé de posséder une solide expérience (environ 5 ans) dans au moins un ou plusieurs domaines liés à la sécurité des systèmes d’information afin de maximiser les apprentissages. Une révision préalable des concepts fondamentaux en sécurité de l’information (gestion des risques, réseaux, architecture, etc.) favorise une meilleure assimilation des contenus. La mise en place d’un plan d’étude personnel et la pratique régulière (lectures, exercices, examens blancs) sont fortement suggérées pour optimiser la préparation à l’examen. Il est conseillé de compléter la formation par des lectures et une pratique continue afin d’approfondir les notions et consolider les compétences acquise

Certifications

Préparation à l'examen CISSP