Plan de cours N° : 1006
Durée : 5 jours (35h)

CISSP
Préparation à la Certification sécurité

PARTICIPANTS / PRE-REQUIS
Consultants, managers, administrateurs réseaux et ingénieurs sécurité. Et plus largement toutes personnes qui souhaitent progresser dans leur carrière actuelle en sécurité informatique.

Avoir une expérience dans l'administration des systèmes, une bonne compréhension des systèmes Unix/Linux et Windows. Au moins cinq ans d'expérience dans le domaine de l'infrastructure informatique et de la cybersécurité seront appréciées.

OBJECTIFS PEDAGOGIQUES
Gérer les identités et des accès (IAM). Evaluer et tester la sécurité. Gérer la sécurité et les risques. Mener des opérations de sécurité. Sécuriser les actifs. Sécuriser le développement de logiciels. Concevoir une architecture et ingénierie de la sécurité. Sécuriser les communications et les réseaux.

MOYENS PEDAGOGIQUES
Tour de table au début de chaque formation pour définir les objectifs de chaque participant,
Alternance entre apports théoriques et exercices pratiques,
Utilisation de cas concrets issus de l'expérience professionnelle de nos formateurs,
Remise d'un support de cours,
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS
Positionnement préalable oral ou écrit,
Evaluation des acquis tout au long de la formation par des exercices de synthèse,
Attestation de stage remise à chaque apprenant, avec son niveau d'acquisition pour chaque objectif pédagogique,
Feuille de présence signée par demi-journée,
Questionnaire de satisfaction pour évaluer la qualité de l'enseignement.
Ce cours vous prépare à l'examen 2024 ISC(2) CISSP-Certified Information Systems Security Professional. Sachant que l'examen lui-même ne fait pas partie de ce cours.

MOYENS TECHNIQUES EN PRESENTIEL
Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs récents et performants, d'un vidéo projecteur et d'un tableau blanc.

MOYENS TECHNIQUES DES CLASSES A DISTANCE
Grâce à un logiciel comme Teams, suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
Nous vous conseillons très fortement l'utilisation de votre webcam et de disposer d'un double écran.
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 04.76.41.14.20.

ORGANISATION
Les cours ont lieu de 9h00-12h30 13h30-17h00 (adaptable à la demande).

PROFIL FORMATEUR
Nous recrutons méticuleusement nos formateurs selon 3 critères: expertise, pédagogie et agilité.

ACCESSIBILITE
Les personnes atteintes de handicap souhaitant suivre nos formations sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités d'organisation.

MISE A JOUR
15/05/2025

Plan de cours N° : 1006
Durée : 5 jours (35h)

CISSP
Préparation à la Certification sécurité

La gouvernance de la sécurité à travers les principes et les politiques
- Sécurité 101
- Comprendre et appliquer les concepts de sécurité
- Les limites de la sécurité
- Évaluer et appliquer les principes de gouvernance de la sécurité
- Gérer la fonction de sécurité
- Politique de sécurité, normes, procédures et lignes directrices
- Modélisation des menaces
- Gestion des risques de la chaîne d'approvisionnement

Concepts de sécurité du personnel et de gestion des risques
- Politiques et procédures de sécurité du personnel
- Comprendre et appliquer les concepts de gestion des risques
- Ingénierie sociale
- Établir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

Planification de la continuité des activités
- Planification de la continuité des activités
- Portée et planification du projet
- Analyse de l'impact sur l'entreprise
- Planification de la continuité, approbation et mise en œuvre du plan

Lois, réglementations et conformité
- Catégories de lois
- Lois nationales sur la protection de la vie privée
- Conformité
- Contrats et marchés publics

Protection de la sécurité des actifs
- Identifier et classer les informations et les biens
- Établir les exigences en matière de traitement des informations et des biens
- Méthodes de protection des données
- Comprendre les rôles des données
- Utilisation des lignes de base de sécurité

Cryptographie et algorithmes à clé symétrique
- Fondements de la cryptographie
- Cryptographie moderne
- Cryptographie symétrique
- Cycle de vie de la cryptographie

ICP et applications cryptographiques
- Cryptographie asymétrique
- Fonctions de hachage
- Signatures numériques
- Infrastructure à clé publique
- Gestion des clés asymétriques
- Cryptographie hybride
- Cryptographie appliquée
- Attaques cryptographiques

Principes des modèles, de la conception et des capacités de sécurité
- Principes de conception sécurisée
- Techniques pour garantir la CIA
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les contrôles sur la base des exigences de sécurité des systèmes
- Comprendre les capacités de sécurité

Plan de cours N° : 1006
Durée : 5 jours (35h)

CISSP
Préparation à la Certification sécurité

Vulnérabilités, menaces et contre-mesures en matière de sécurité

- Responsabilité partagée
- Localisation et souveraineté des données
- Évaluer et atténuer les vulnérabilités des architectures de sécurité, des conceptions et des éléments de solution
- Systèmes basés sur les clients
- Systèmes basés sur des serveurs
- Systèmes de contrôle industriel
- Systèmes distribués
- Systèmes de calcul à haute performance (HPC)
- Systèmes d'exploitation en temps réel
- Internet des objets, Informatique en périphérie et Fog Computing
- Dispositifs embarqués et systèmes cyber-physiques
- Microservices
- Infrastructure en tant que code
- Architecture immuable
- Systèmes virtualisés
- Conteneurisation
- Dispositifs mobiles
- Mécanismes essentiels de protection de la sécurité
- Défauts et problèmes courants de l'architecture de sécurité

Exigences en matière de sécurité physique

- Appliquer les principes de sécurité à la conception du site et de l'installation
- Mettre en œuvre les contrôles de sécurité du site et de l'installation
- Mettre en œuvre et gérer la sécurité physique

Architecture et composants d'un réseau sécurisé

- Modèle OSI
- Modèle TCP/IP
- Analyse du trafic réseau
- Protocoles communs de la couche application
- Protocoles de la couche transport
- Système de noms de domaine
- Protocole Internet (IP)
- Problèmes liés à l'ARP
- Protocoles de communication sécurisés
- Implications des protocoles multicouches
- Segmentation
- Réseaux périphériques
- Réseaux sans fil
- Communications par satellite
- Réseaux cellulaires
- Réseaux de distribution de contenu (CDN)
- Composants des réseaux sécurisés

Communications sécurisées et attaques sur les réseaux

- Mécanismes de sécurité des protocoles
- Communications vocales sécurisées
- Gestion de la sécurité de l'accès à distance
- Collaboration multimédia
- Surveillance et gestion
- Équilibrage de charge
- Gestion de la sécurité du courrier électronique
- Réseau privé virtuel
- Commutation et réseaux locaux virtuels
- Traduction d'adresses de réseau
- Connectivité avec des tiers
- Technologies de commutation
- Technologies WAN
- Liaisons par fibre optique
- Prévenir ou atténuer les attaques du réseau

Plan de cours N° : 1006
Durée : 5 jours (35h)

CISSP
Préparation à la Certification sécurité

Gestion de l'identité et de l'authentification
- Contrôler l'accès aux ressources
- Le modèle AAA
- Mise en œuvre de la gestion des identités
- Gestion du cycle de vie du provisionnement des identités et des accès

Contrôle et surveillance des accès
- Comparaison des modèles de contrôle d'accès
- Mise en œuvre des systèmes d'authentification
- Application de la politique d'accès de confiance zéro
- Comprendre les attaques de contrôle d'accès

Évaluation et test de la sécurité
- Mise en place d'un programme d'évaluation et de test de la sécurité
- Évaluer les vulnérabilités
- Tester vos logiciels
- Formation et exercices
- Mise en œuvre des processus de gestion de la sécurité et collecte des données relatives aux processus de sécurité

Gestion des opérations de sécurité
- Appliquer les concepts fondamentaux des opérations de sécurité
- Assurer la sécurité du personnel
- Fournir des informations et des actifs en toute sécurité
- Services gérés dans le cloud
- Effectuer la gestion de la configuration (CM)
- Gérer les changements
- Gérer les correctifs et réduire les vulnérabilités

Prévenir les incidents et y répondre
- Gestion des incidents
- Mise en œuvre de mesures de détection et de prévention
- Journalisation et surveillance
- Automatisation de la réponse aux incidents

Planification de la reprise après sinistre
- La nature du sinistre
- Comprendre la résilience des systèmes, la haute disponibilité et la tolérance aux pannes
- Stratégie de reprise
- Élaboration d'un plan de reprise
- Formation, sensibilisation et documentation
- Tests et maintenance

Enquêtes et éthique
- Enquêtes
- Principales catégories de délits informatiques
- Éthique

Sécurité du développement de logiciels
- Introduction des contrôles de développement de systèmes
- Mise en place de bases de données et d'entrepôts de données
- Menaces sur le stockage
- Comprendre les systèmes basés sur la connaissance

Attaques contre les codes malveillants et les applications
- Les logiciels malveillants
- Prévention des logiciels malveillants
- Attaques d'applications
- Vulnérabilités d'injection
- Exploitation des vulnérabilités d'autorisation
- Exploitation des vulnérabilités des applications Web
- Contrôles de sécurité des applications
- Pratiques de codage sécurisées