CERTIFICATION CISSP® : PREPARATION À L'EXAMEN

Public	Cette formation est destinée aux personnes préparant l'examen (ISC)2 CISSP.
Durée	5 jours - 35 heures
Pré-requis	Les candidats CISSP doivent posséder certain prérequis établis par l'(ISC)2. Veuillez vous référer au site internet de l'(ISC)2 à l'adresse suivante:https://www.isc2.org/cissp/default.aspx.
Objectifs	Learning Tree a développé la formation 2058 pour aider les participants à se préparer de manière stratégique à l'examen (ISC)2® CISSP® (Certified Information Systems Security Professional). Elle comprend des activités et des exercices pratiques visant à renforcer la compréhension des dix domaines CBK. Elle est dispensée par des formateurs Learning Tree qui détiennent une certification CISSP en cours de validité et sont des leaders dans l'industrie de la sécurité de l'information. Elle vous permet d'identifier les domaines majeurs que vous devez étudier et comprend : Des techniques pédagogiques avancées Une évaluation avant et après séminaire Un exemplaire de The Official (ISC)2® Guide to the CISSP® CBK®, Third Edition
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

PROTÉGER LES INFORMATIONS EN APPLIQUANT DES ALGORITHMES MATHÉMATIQUES ET LA TRANSFORMATION DES DONNÉES

- Systèmes de cryptographie symétrique et asymétrique
- S'assurer de l'intégrité des messages via le hachage
- Authenticité des messages avec les signatures numériques

DÉCOUVRIR LES MENACES DES SYSTÈMES DE CHIFFREMENT

- Revoir les attaques cryptanalytiques
- Reconnaître les attaques d'analyse statistique

MÉCANISMES POUR PROTÉGER LES SYSTÈMES D'INFORMATION

- Définir les contrôles administratifs, techniques et physiques
- Mettre en œuvre des approches centralisées et décentralisées
- Examiner les authentifications biométriques et à facteurs multiples

ATTAQUES DES CONTRÔLES D'ACCÈS

- Identifier les menaces courantes, différencier les systèmes de détection et les systèmes de protection

EXAMINER LES MODÈLES ET LES FRAMEWORKS DE SÉCURITÉ

- Triade de la sécurité de l'information et modèles multi-niveau
- Examiner les normes du marché : ISO 27001/27002

CONCEPTS DE LA SÉCURITÉ DES SYSTÈMES ET DES COMPOSANTS

- Principes et défauts de la conception des systèmes
- Modèles et critères de certification et d'accréditation

SÉCURISER LE CYCLE DE VIE DU DÉVELOPPEMENT DE LOGICIEL

- Méthodes et les contrôles du développement de logiciel
- Mettre en évidence les menaces de codage : Cross-Site Scripting (XSS), attaques JavaScript et Buffer Overflow

TRAITER LES PROBLÈMES ET LES CONCEPTS DE LA SÉCURITÉ DES BASES DE DONNÉES

- Identifier les menaces et les attaques de bases de données
- Définir les caractéristiques de la conception de BdD sécurisées

JURIDIQUE, RÉGULATIONS, ENQUÊTES ET CONFORMITÉ ANALYSER LES MESURES ET LES TECHNIQUES JURIDIQUES

- Revoir la propriété intellectuelle, la responsabilité et les lois
- Différencier le crime traditionnel du crime informatique

ADOPTER UN COMPORTEMENT ÉTHIQUE ET RESPECTER LA CONFORMITÉ

- Le $(ISC)^2$ Code of Professional Ethics
- Exigences et procédures de conformité

RENDRE LA SÉCURITÉ CONFORME AUX OBJECTIFS DE L'ENTREPRISE

- Utiliser les principes de sécurité fondamentaux
- Gérer les stratégies, les normes et les procédures de sécurité

APPLIQUER LES CONCEPTS DE GESTION DES RISQUES

- Evaluer les menaces et les vulnérabilités
- Réaliser une analyse et un contrôle des risques

PRÉSERVER L'ACTIVITÉ

- Adhérer au Business Continuity Management Code of Practice and Specifications (BS 25999)
- Analyse d'impact

DÉVELOPPER UNE STRATÉGIE DE REPRISE

- Concevoir un plan de reprise après sinistre
- Mettre en œuvre les processus de test et de maintenance

DÉFINIR UNE ARCHITECTURE RÉSEAU SÉCURISÉE

- TCP/IP et autres modèles de protocoles
- Se protéger des attaques réseau

EXAMINER LES LES RÉSEAUX ET LES COMPOSANTS SÉCURISÉS

- Technologies filaires et sans fil
- Pare-feu, proxies et tunnels
- Identifier le bon usage du chiffrement

MAINTENIR LA RÉSILIENCE OPÉRATIONNELLE

- Protéger les atouts de valeur
- Contrôler le système et les comptes utilisateur
- Gérer les services de sécurité de façon efficace

SAUVEGARDER LES RESSOURCES PHYSIQUES

- Refuser les accès non autorisés
- Concevoir des environnements résistant aux hostilités et menaces des catastrophes naturelles

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 03/04/2020