Normes et méthodes

Préparation à la certification CCSP

5 jours (35h00) | ★★★★½ 4,6/5 | CERT-CCSP | Certification CCSP (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 05/06/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire les composants physiques et virtuels et identifier les principales technologies des systèmes basés sur le Cloud
- Définir les rôles et les responsabilités des clients, des fournisseurs, des partenaires, des courtiers et des divers professionnels techniques qui prennent en charge les environnements Cloud Computing
- Identifier et expliquer les cinq caractéristiques requises pour répondre à la définition du NIST (National Institute of Standards and Technology) du Cloud Computing
- Différencier les modèles de prestation de services et les frameworks qui sont incorporés dans l'architecture de référence du Cloud Computing
- Discuter des stratégies de sauvegarde des données, de classification des données, de protection de la confidentialité, de conformité avec les organismes de réglementation et de collaboration avec les autorités lors d'enquêtes judiciaires
- Différencier l'analyse forensic dans les Data Centers d'entreprise et les environnements Cloud Computing
- Evaluer et mettre en oeuvre les contrôles de sécurité nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité dans le cadre du Cloud Computing
- Identifier et expliquer les six phases du cycle de vie des données
- Expliquer les stratégies de protection des données au repos et des données en mouvement
- Décrire le rôle du cryptage dans la protection des données et les stratégies spécifiques de gestion des clés
- Comparer diverses stratégies Business Continuity et Disaster Recovery basées sur le Cloud et sélectionner une solution appropriée aux besoins spécifiques de l'entreprise
- Comparer les aspects de sécurité du SDLC (Software Development Life Cycle) dans les environnements standard du Data Center et du Cloud Computing
- Décrire comment les solutions de gestion des identités fédérées et des accès atténuent les risques dans les systèmes du Cloud Computing
- Effectuer une analyse des écarts entre les pratiques de référence et les bonnes pratiques du secteur
- Développer des SLA (Service Level Agreements) pour les environnements Cloud Computing
- Réaliser des évaluations de risques des environnements Cloud existants et proposés
- Enoncer les normes professionnelles et éthiques de (ISC)² et de la certification CCSP.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir un minimum de cinq années cumulées d'expérience professionnelle rémunérée dans le domaine des technologies de l'information, dont trois ans en sécurité de l'information et un an dans un ou plusieurs des six domaines de la norme CCSP CBK, ou être certifié CISSP.

Public concerné

Architectes d'entreprise, architectes / administrateurs / ingénieurs / consultants / responsables de sécurité, ingénieurs / architectes systèmes.

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 M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Concepts, architecture et conception du Cloud

- Comprendre les concepts du Cloud Computing
- Décrire l'architecture Cloud de référence
- Comprendre les concepts pertinents de sécurité liés au Cloud Computing
- Comprendre les principes de conception du Cloud Computing sécurisé
- Evaluer les fournisseurs de services Cloud

Sécurité des données dans le Cloud

- Décrire les concepts de données Cloud
- Concevoir et mettre en oeuvre des architectures de stockage de données dans le Cloud
- Concevoir et appliquer des technologies et des stratégies de sécurité des données
- Mettre en oeuvre la Data Discovery
- Planifier et mettre en oeuvre la classification des données
- Concevoir et mettre en oeuvre la gestion des droits à l'information (Information Rights Management)
- Planifier et mettre en oeuvre des politiques de conservation, de suppression et d'archivage des données
- Concevoir et mettre en oeuvre l'auditabilité, la traçabilité et la responsabilité des évènements liés aux données

Cloud Platform et la sécurité de l'infrastructure

- Comprendre l'infrastructure Cloud et les composants de la plateforme
- Concevoir un Data Center sécurisé
- Analyser les risques associés avec l'infrastructure et les plateformes Cloud
- Planifier et mettre en oeuvre des contrôles de sécurité
- Planifier le Business Continuity (BC) et le Disaster Recovery (DR)

Sécurité des applications Cloud

- Préconiser la formation et la sensibilisation à la sécurité des applications
- Décrire le processus Secure Software Development Life Cycle (SDLC)
- Appliquer le SDLC
- Appliquer l'assurance et la validation des logiciels Cloud
- Utiliser des logiciels sécurisés vérifiés
- Comprendre les spécificités de l'architecture des applications Cloud
- Concevoir des solutions appropriées IAM (Identity and Access Management)

Opérations de sécurité du Cloud

- Construire et mettre en oeuvre l'infrastructure physique et logique pour l'environnement Cloud
- Exploiter et maintenir l'infrastructure physique et logique pour l'environnement Cloud
- Mettre en oeuvre des contrôles et des normes opérationnels
  - Information Technology Infrastructure Library (ITIL)
  - International Organization for Standardization / International Electrotechnical Commission (ISO/IEC 20000-1)
- Soutenir le Digital Forensics
- Gérer la communication avec les parties concernées
- Gérer les opérations de sécurité

Juridique, risques et conformité

- Articuler les exigences légales et les risques uniques au sein de l'environnement Cloud

- Comprendre les problèmes de confidentialité
- Comprendre le processus d'audit, les méthodologies et les adaptations nécessaires pour un environnement Cloud
- Comprendre les implications Cloud pour la gestion des risques de l'entreprise
- Comprendre l'externalisation et la conception de contrats Cloud

Passage de la certification

- Cette formation comprend le voucher nécessaire à l'inscription et au passage (ultérieur) de l'examen
- Ce dernier ne pourra être passé qu'en présentiel uniquement, dans un centre Pearson Vue Select agréé
- L'examen (en anglais) s'effectue en ligne et durera en moyenne 3h00
- Il s'agit d'un QCM de 125 questions (70% de bonnes réponses sont nécessaires pour l'obtention de la certification)

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par une certification éditeur, et/ou un questionnaire d'auto-évaluation

Les + de la formation

Un minimum de 4 personnes sera nécessaire pour maintenir la session.

De plus, il est très important de noter que pour chaque inscription, un délai de 10 jours (minimum) est imposé par l'éditeur avant d'obtenir les documents pédagogiques (donc pas d'inscription possible à moins de 10 jours).

Le support de cours est en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme.
Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.