

Professional Cloud Security Manager

Référence : CCC-PCS

Durée : 3 jours

Certification : PCS

CONNAISSANCES PREALABLES

- • Aucun prérequis mais il est souhaitable d'avoir 5 ans d'expérience dans la sécurité des entreprises et une bonne compréhension des services du Cloud Computing et des modèles de déploiement. .

PROFIL DES STAGIAIRES

- Administrateur/Ingénieur réseau. • Auditeur des services Cloud Computing. • CDO (Chief Digital Office). • Consultants et opérationnels IT. • Professionnels du risque et de la conformité. • Professionnels Sécurité IT.

OBJECTIFS

- Appliquer les meilleures pratiques de règles de gouvernance et de sécurité . • Comprendre, appliquer et analyser comment gérer l'accès aux ressources Cloud, des méthodes pour sécuriser les data, operating systèmes, les applications, l'infrastructure Cloud. • Expliquer ce qui sécurise les différents services Cloud et les modèles de déploiement. • Expliquer le design sécurité au regard de l'infrastructure, des configurations et des applications . • Passer dans les conditions optimales la certification internationale «Professional Cloud Security Manager».

CERTIFICATION PREPAREE

Professional Cloud Security Manager

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Cloud

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Sécurité, risques et gouvernance

- Les concepts, la gestion de la sécurité IT, la gouvernance IT, la sécurité du Cloud Computing
- Implémentation des traitements et mitigations de risque Cloud, les impacts business et techniques sur la politique de gouvernance

Les menaces de sécurité et les défis

- Différence de gouvernance traditionnelle et Cloud, les différences entre la sécurité partagée et le modèle de conformité dans le Cloud
- Les risques et les impacts en termes business et technique et leurs conséquences sur la politique de

gouvernance technique : protection/classification des data, modèles de menaces, ISA

- SLA
- Asset partagés

Gestion de Sécurité dans le Cloud

- Classification des données et son importance
- Les risques et les mesures pour réduire les menaces de sécurité
- La confidentialité et la gestion/implémentation des identités (IAM)
- Les problématiques d'accès, de confidentialité, de risque et de conformité
- Les modèles de services et de déploiement qui impactent la valeur business

Légal, contractuel et monitoring opérationnel dans le Cloud

- Concepts
- Les défis
- Implémentation des mitigations liées aux éléments clés légaux
- Risques et opportunités des services monitorés cloud

Gestion du réseau de sécurité dans le Cloud

- La gestion de la vulnérabilité et l'architecture sécurité au regard du Cloud et de son rôle
- SDN
- NVS
- Les avantages de la virtualisation, la gestion Patch et les tests de pénétration

Continuité du business, restauration de désastre et planning de performance et de capacité

- Concepts de la continuité business (BC) et de la restauration du désastre (DR)
- Les défis
- L'implémentation de la capacité dans le BC et DR, les risques et opportunités, le concept de la planification de la Capacité et de la Performance
- Les risques et opportunités

- Le concept de la planification de la Capacité et de la Performance

Pratiques de gestion de sécurité cloud avancée

- Spécificité sur les enjeux de la gouvernance et de la sécurité sur un modèle PaaS
- Prise de conscience des enjeux de sécurité et de gouvernance pour concevoir et gérer les systèmes PaaS
- Développement standard
- Sécurité API

Planning de sécurité, standards et évolution du cloud

- Process de sécurité et enjeux des software, application et services opérées dans le cloud
- Planning
- Contrôle et audit et évolution de la sécurité du cloud

Révisions et passage de l'examen final en fin de formation (voir le déroulement de l'examen)