DAWAN
Plan de la formation
www.dawan.fr

Formation Cloud avancé : Professional Manager Sécurité (PCS)

Durée :	3 jours
Public :	Spécialiste du Cloud Computing, Manager sécurité IT, Consultant en sécurité IT, Auditeurs informatiques.
Pré-requis :	Même si cela n'est pas obligatoire, il est fortement recommandé d'avoir obtenu préalablement la certification « Cloud Technology Associate ».
Objectifs :	- Connaître les principes de Sécurité et gouvernance ainsi que les défis du Cloud Computing - Savoir comment gérer la sécurité dans le Cloud - Savoir gérer des contrats Cloud, leurs termes et les conditions juridiques - Connaître les politiques de sécurité et de gouvernance (IaaS, PaaS, SaaS) - Appréhender la continuité métier et Cloud.
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	CLO100502-F
Note de satisfaction des participants:	Pas de données disponibles

Introduction

Comment sécuriser les services Cloud et les modèles de déploiement ?
Concevoir la sécurité d'un Cloud au niveau de l'infrastructure, des configurations et des applications,
Gestion des accès aux ressources en utilisant des comptes, des groupes…
Moyens de sécurisation des données, systèmes d'exploitation, des applications… dans le Cloud.

Sécurité, Gouvernance et risques

Concepts de GRC (Gouvernance, Risque et Conformité),
Concepts de sécurité sous-jacents (CIA),
Mise en œuvre des mesures de traitement et de réduction de risque dans le Cloud,
Terminologies utilisées pour décrire les menaces et problèmes de sécurité en Cloud.

Menaces de sécurité et challenge

Différences entre GRC traditionnel et GRC Cloud,
Différences en sécurité et conformité en Cloud,
Mise en œuvre de modèle de conformité et de sécurité,
Risques et impacts en terme de :
Sécurité métiers et techniques,
Effets sur les gouvernances et politiques métiers et techniques.

La gestion de la sécurité en Cloud

Concept de classification des données,
Gestion des identités et accès (IAM) :
L'importance d'avoir et d'utiliser un framework IAM,
Bénéfices (e.g. automatisation, rationalisation et self-service),
L'IAM pour le cloud.
Risques et impacts de la protection de données,
Les différents types de mise en œuvre réutilisables pour sécuriser les données dans le Cloud

Surveillance opérationnelle, contractuelle et légale en Cloud

Dispositifs légaux et de régulation liés au Cloud,
Challenges légaux et mesures de mitigation,
Risques et opportunités liés à la supervision des services Cloud,
Terminologies utilisées pour décrire les menaces et problèmes de sécurité en Cloud.

Gestion de la sécurité réseau en Cloud

Principes de sécurité réseau,
Gestion des vulnérabilités et architecture de la sécurité.

Continuité métier, Reprise sur sinistre et Planification des capacités et performance

Concepts de continuité métier et reprise sur sinistre,
Challenges associés en environnement traditionnel et en Cloud
Risques et opportunités de solutions BC/DR en Cloud,
Planning des capacités et des performances Cloud.

Pratiques avancées associées à la gestion de la sécurité en Cloud

Problèmes spécifiques de sécurité et de gouvernance du modèle PaaS,
Mécanismes de sensibilisation associés pour concevoir et gérer les systèmes PaaS.

Plan de sécurité, standards et évolution du Cloud

Analyse du processus de sécurité et problèmes associés pour les applications et services exploités en Cloud,
Application du processus de sécurité et problèmes associés aux connaissances de conception et de gestion des systèmes applicatifs,
Planifier la sécurité du Cloud,
Standards, contrôles et audits Cloud,
Evolution de la sécurité du Cloud.

Préparation à l'examen « Professional Cloud Security Manager (PCS) »,

Passage de l'examen « Professional Cloud Security Manager (PCS) ».