Sparks.

Programme de formation

Certification PCS Professional Cloud Seciruty Manager

• Objectifs

Notre formation PCS couvre les principes fondamentaux de sécurité, risques et mise en conformité en environnement cloud tels qu'ils sont décrits par le CCC (Cloud Credential Council). Vous apprendrez à appliquer les concepts de sécurité essentiels et saurez identifier les risques et impacts liés au cloud computing. Formez-vous efficacement et soyez prêts à relever les défis de sécurité business et techniques sous-jacents à la mise en place d'une solution cloud. A l'issue de notre formation, les participants passeront la certification PCS Professional Cloud Security Manager, administrée par le Cloud Credential Council (CCC). L'examen s'effectuera durant la dernière journée de formation, en ligne et en anglais (temps additionnel et dictionnaire bilingue autorisé pour les non-anglophones), sous la supervision d'un formateur accrédité.

• Pré requis

Une expérience dans la sécurité est souhaitable. Il est également recommandé d'avoir suivi le cours Cloud Technology Associate (CTA) ou de posséder des connaissances équivalentes.

• Durée

3 jours

• Public

Analystes, Auditeurs, Consultants, Responsable sécurité, Risk managers

•Plan de formation

Introduction à la formation PCS
Vue d'ensemble du Cloud Computing
Rappels des concepts fondamentaux
Sécuriser les différents modèles de service et de déploiement du cloud
Concevoir une infrastructure, des configurations et des applications (architecture de sécurité)
Gérer les accès aux ressources
Outils de sécurisation des ressources du cloud
Bonnes pratiques

Sécurité, gouvernance et risques
Terminologie, concepts : gouvernance, risque, conformité
Principe CIA (Confidentialité, intégrité et disponibilité)
Cycles de vie de la gestion des risques et de la sécurité des données
Plans de traitement et réduction des risques
Eléments de risques selon les modèles de service
Impacts business et techniques sur la politique de gouvernance

Menaces et défis pour la sécurité en environnement Cloud
Spécificités pour la sécurité et conformité (GRC) en environnement Cloud
Mise en œuvre d'un modèle de sécurité et de conformité
Risques et impacts pour le business et la technique
Effets sur la politique de gouvernance technique
Protection, classification des données
Modèles de menaces
Information Service Agreement (ISA), Service Level Agreement (SLA)

Gestion de la sécurité
Gestion des identités et des accès (IAM) dans le cloud
Utiliser un framework d'entreprise pour l'IAM
Classifier, manipuler et protéger les données, importance dans le cloud
Cycle de vie de la sécurité des données
Mesures pour réduire les menaces de sécurité
Impacts de la protection des données
Types d'implémentation de sécurité réutilisés pour sécuriser les données dans le cloud

Monitoring légal, contractuel et opérationnel
Dispositifs légaux et réglementaires : vue d'ensemble
Principales considérations, défis, risques et opportunités liés à la supervision de services cloud
Mesures d'atténuation liées aux éléments juridiques clés
Terminologies pour la sécurité dans le cloud
Surveillance des fournisseurs et consommateurs
Opérations de sécurité

Gestion de la sécurité réseau
Concepts de base pour la sécurité du réseau en environnement cloud
Software-Defined Networking (SDN)
Network Service Virtualization (NSV)
Vulnérabilité, gestion des patchs et tests d'intrusion (pentest)
Architecture de la sécurité cloud

Continuité business, reprise après sinistre et planification
Principes de la continuité des activités (business continuity)
Technologie résiliente de la reprise après sinistre (disaster recovery)
Défis, risques et opportunités associés dans un environnement cloud
Planification des capacités et performances

Pratiques avancées de gestion de la sécurité
Sécurité dans la virtualisation, conteneurs
Normes de développement sécurisé pour le cloud
Planification de la sécurité cloud
Contrôles et audits
Evolution et perspectives pour la sécurité cloud

Passage de l'examen de certification PCS
Révisions et examen blanc, correction commentée
Trucs et astuces pour réussir l'examen
Modalités d'évaluation : 25 questions basées sur un scénario, 75 minutes (15 minutes additionnelles pour les non-anglophones), obtention de la certification avec 65% de bonnes réponses.