Date de publication : 22/02/2024

Formation : Oracle Cloud Infrastructure Security Live Class

COURS OFFICIEL : SUPPORT NUMERIQUE ACCESSIBLE UNIQUEMENT PENDANT 90 JOURS

Cours pratique - 4j - 28h00 - Réf. OCS

Avec cette formation, vous acquérez une expérience pratique de l'utilisation de la sécurité réseau, du coffre-fort, de la clé de cryptage principale, du coffre-fort des données, du pare-feu d'application web, de Cloud Guard, des zones de sécurité et bien plus encore.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Gérer des identités et des accès
- Sécuriser des applications
- Sécuriser des données et des bases de données
- Sécuriser des réseaux et des ordinateurs

Public concerné

Administrateur sécurité.

Prérequis

Avoir suivi la formation Oracle Cloud Infrastructure Foundations ou disposer de connaissances et compétences équivalentes.

Certification

La réussite de l'examen permet d'obtenir la certification Oracle Cloud Platform Identity and Security Management 2022 Professional.
Comment passer votre examen ?

PARTICIPANTS

Administrateur sécurité.

PRÉREQUIS

Avoir suivi la formation Oracle Cloud Infrastructure Foundations ou disposer de connaissances et compétences équivalentes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours et travaux pratiques en anglais, au format numérique et ACCESSIBLE UNIQUEMENT PENDANT 90 JOURS. Bonne compréhension de l'anglais à l'écrit.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

Programme de la formation

1 Introduction à la sécurité

- Modèle de sécurité partagé.
- Sécurité Zero Trust.
- Conception et contrôles de sécurité.
- Présentation des services de sécurité.

2 Gestion des identités et des accès

- Domaines d'identité.
- AuthN.
- AuthZ.
- Politiques communes.
- Compartiments.
- Héritage et attachement des politiques.
- Politiques conditionnelles.
- Politiques avancées.
- Sources réseau.
- Contrôle d'accès basé sur des balises.
- Groupes dynamiques.
- Fédération.
- Comprendre les options de connexion.

3 Sécurité des infrastructures – Réseau

- Introduction au réseau cloud virtuel.
- Sécurité du réseau cloud virtuel.
- Sécurité VCN – Listes de sécurité, démo NSG.
- Connectivité VCN.
- Réseau cloud virtuel – Peering.
- Service DNS.
- Stratégies IAM pour les administrateurs/utilisateurs réseau.
- Load Balancer.
- Gestion SSL.
- Bastion.

4 Sécurité des infrastructures – Calcul

- Meilleures pratiques de calcul.
- Gestion du système d'exploitation avec Oracle Cloud Infrastructure.
- Hôtes dédiés de machines virtuelles.
- Analyse des vulnérabilités.
- Sécurité pour OKE.
- Politiques IAM et RBAC.
- Les secrets de Kubernetes.
- Sécurité des clusters.
- Sécurité du pool de nœuds.
- Sécurité Internet.
- Considérations multilocataires.
- Sécurité des images.
- Sécurité pour les fonctions Oracle.

5 Sécurité des données et des bases de données

- Bases du chiffrement.
- Présentation du coffre-fort.
- Clés d'importation et d'exportation.
- Intégration des services OCI avec Vault.
- Sauvegarder et répliquer les coffres-forts et les clés.
- Secrets.
- Données sécurisées.
- Stockage.
- Gestion de l'accès et de l'authentification.
- La gestion du cycle de vie.
- Réplication du stockage d'objets et copie entre régions.
- Gestion des versions
- La conservation des données.
- Enregistrement.
- Stockage de fichiers.
- Sécurité : Stockage de fichiers.
- Bloquer le stockage.
- Sécurité de la base de données Oracle.

6 Sécurité des applications

- Sécuriser les applications dans le cloud.

7 Passerelle API

- Groupes de sécurité réseau.
- Prise en charge de TLS mutuel (mTLS).
- Custom Trust Store.

8 Créer et gérer des certificats

- Présentation des certificats.

9 Gestion de la posture de sécurité du cloud

- Qu'est-ce que la gestion de la posture de sécurité du cloud ?.
- Activer Cloud Guard.
- Concepts de protection du cloud
- Problèmes de garde cloud.
- Cloud Guard – Gérer les recettes du détecteur.
- Recettes de répondeur Cloud Guard
- Notifications Cloud Guard.
- Zones de sécurité et conseiller en sécurité.

10 Opérations de sécurité

- Gestion des opérations de sécurité.
- Surveillance.
- Service de journalisation.
- Ingestion de journaux pour Analytics.
- Informations avec Logging Analytics.
- Service de vérification.
- Service d'événements.
- Conformité réglementaire.