EduGroupe
Accompagner pour réussir

Sécurité du Cloud Computing

Durée : 2 jours (14 heures)

CONNAISSANCES PREALABLES

- Connaissances générales des systèmes d'information et des réseaux.
- Connaissances de base des architectures Cloud (IaaS, PaaS, SaaS).
- Une expérience en administration système ou en exploitation d'infrastructures informatiques est recommandée.

PROFIL DES STAGIAIRES

- Administrateurs systèmes et réseaux
- Administrateurs Cloud
- Ingénieurs infrastructures et exploitation
- Architectes techniques
- Responsables cybersécurité
- RSSI et correspondants sécurité
- Consultants et chefs de projets techniques
- Toute personne impliquée dans le déploiement ou l'exploitation d'environnements Cloud.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre les enjeux de sécurité propres aux environnements Cloud.
- Identifier les risques associés aux modèles IaaS, PaaS et SaaS.
- Maîtriser le modèle de responsabilité partagée entre fournisseur et client.
- Mettre en œuvre les bonnes pratiques de sécurisation des infrastructures Cloud.
- Renforcer la gestion des identités, des accès et des données dans le Cloud.
- Détecter les principales vulnérabilités et erreurs de configuration.
- Intégrer les exigences de conformité et de gouvernance dans les projets Cloud.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Alternance d'apports théoriques et de retours d'expérience issus de projets Cloud réels.
- Études de cas inspirées d'incidents de sécurité ayant affecté des environnements Cloud.
- Ateliers collaboratifs d'analyse des risques et de sécurisation d'architectures Cloud.
- Exercices de configuration et de contrôle des accès.
- Analyse de scénarios d'attaques et de compromission.
- Échanges de bonnes pratiques et retours d'expérience des participants.

FORMATEUR

- Consultant expert en cybersécurité et sécurité Cloud disposant d'une expérience significative dans la conception, le déploiement et la sécurisation d'environnements Cloud publics, privés et hybrides.

METHODE D'EVALUATION DES ACQUIS

- Questionnaire de positionnement en début de formation.
- Validation progressive des acquis à travers les ateliers et études de cas.
- Exercices pratiques d'analyse des risques et de sécurisation.
- Quiz de validation des connaissances.
- Cas pratique de synthèse en fin de formation.
- Questionnaire d'évaluation des acquis en fin de parcours.

CONTENU DU COURS

Jour 1 : Comprendre les enjeux de sécurité du Cloud et protéger les accès (7h)

Module 1 : Introduction à la sécurité du Cloud Computing (2h)

Objectifs

- Comprendre les spécificités de la sécurité dans le Cloud.
- Identifier les risques liés aux différents modèles de services Cloud.

Contenu

- Définitions et concepts du Cloud Computing.
- Modèles IaaS, PaaS et SaaS.
- Cloud public, privé et hybride.
- Enjeux de sécurité liés à la migration vers le Cloud.
- Panorama des menaces actuelles.
- Principaux incidents de sécurité observés dans les environnements Cloud.

Mise en pratique

Brainstorming collectif :

- Identification des risques liés à l'adoption du Cloud dans une organisation.
- Analyse d'incidents réels ayant conduit à des fuites ou compromissions de données.

Module 2 : Comprendre le modèle de responsabilité partagée (1h30)

Objectifs

- Identifier les responsabilités respectives du fournisseur Cloud et du client.
- Comprendre les impacts de ce modèle sur la gouvernance de la sécurité.

Contenu

- Principe de responsabilité partagée.
- Répartition des responsabilités selon les modèles IaaS, PaaS et SaaS.
- Limites des garanties apportées par les fournisseurs.
- Gouvernance et pilotage des risques.

Mise en pratique

Atelier :

- Cartographie des responsabilités de sécurité dans différents scénarios Cloud.

Module 3 : Gestion des identités et des accès dans le Cloud (2h)

Objectifs

- Sécuriser les accès aux ressources Cloud.
- Réduire les risques liés aux privilèges excessifs.

Contenu

- Gestion des identités (IAM).
- Authentification multifacteur (MFA).
- Gestion des rôles et privilèges.
- Comptes administrateurs et comptes de service.
- Principe du moindre privilège.
- Gestion des accès tiers.

Mise en pratique

Étude de cas :

- Analyse d'une politique IAM présentant plusieurs faiblesses.
- Définition des mesures correctives.

Module 4 : Sécuriser les ressources et configurations Cloud (1h30)

Objectifs

- Identifier les erreurs de configuration les plus fréquentes.
- Appliquer les bonnes pratiques de sécurisation.

Contenu

- Mauvaises configurations courantes.
- Sécurisation du stockage Cloud.
- Contrôle des ressources exposées sur Internet.
- Gestion des configurations et des changements.
- Principes du Cloud Security Posture Management (CSPM).

Mise en pratique

Atelier :

- Analyse d'une architecture Cloud présentant plusieurs erreurs de configuration.

Jour 2 : Protéger les données, superviser et assurer la conformité (7h)

Module 5 : Protection des données dans le Cloud (2h)

Objectifs

- Garantir la confidentialité et l'intégrité des données.
- Sécuriser les échanges et les stockages Cloud.

Contenu

- Classification des données.
- Chiffrement des données au repos et en transit.
- Gestion des clés de chiffrement.
- Sauvegarde et restauration.
- Prévention des pertes de données (DLP).

Mise en pratique

Atelier :

- Définition d'une stratégie de protection des données selon différents niveaux de sensibilité.

Module 6 : Supervision et détection des incidents dans le Cloud (2h)

Objectifs

- Détecter les comportements anormaux.
- Mettre en place une surveillance efficace des ressources Cloud.

Contenu

- Journalisation et traçabilité.
- Collecte des événements de sécurité.

- Surveillance des accès.
- Détection des activités suspectes.
- Intégration avec les solutions SIEM.
- Réponse aux incidents dans le Cloud.

Mise en pratique

Étude de cas :

- Analyse de journaux d'événements Cloud et identification d'indicateurs de compromission.

Module 7 : Gouvernance, conformité et gestion des risques Cloud (2h)

Objectifs

- Intégrer la sécurité dans la gouvernance Cloud.
- Assurer la conformité réglementaire et normative.

Contenu

- Analyse des risques Cloud.
- Gouvernance et politiques de sécurité.
- RGPD et protection des données personnelles.
- Normes ISO 27001, ISO 27017 et ISO 27018.
- Exigences contractuelles et auditabilité.
- Gestion des fournisseurs Cloud.

Mise en pratique

Atelier :

- Réalisation d'une analyse de risques simplifiée pour un projet de migration Cloud.

Module 8 : Cas pratique de synthèse (1h)

Objectifs

- Mettre en application l'ensemble des notions abordées durant la formation.

Mise en pratique

Étude de cas fil rouge :

À partir du projet de migration d'une entreprise vers un environnement Cloud :

- Identification des risques majeurs.
- Définition des responsabilités.
- Sécurisation des accès et des données.
- Mise en place des contrôles de sécurité.
- Élaboration d'un plan d'amélioration de la sécurité Cloud.
- Présentation des recommandations au groupe.

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à mailto:referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.