Formation Sécurité Cloud les fondamentaux

Comprendre les enjeux, moyens, techniques et outils pour assurer une protection optimale sur le cloud

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La formation Cloud Security Fundamentals est une introduction à la sécurité sur le cloud, elle permet aux participants de comprendre et évaluer les nouveaux risques apportés par le cloud afin de les orienter vers une mise en oeuvre d'un programme de sécurité cloud adaptée et basée sur les bonnes pratiques.

Référence	CLOUDSECFND
Durée	1 jour (7h)
Tarif	700 €HT

Objectifs

| Connaître les nouveaux risques apportés par le cloud.
| Connaître les moyens mis en oeuvre par les cloud providers pour la sécurité.
| Connaître les premiers chantiers de sécurité à attaquer lors de la migration sur le cloud
| Connaître les pratiques, les techniques et outils pour assurer une protection optimale sur le cloud.

Prérequis

| Des connaissances de base sur le cloud computing sont nécessaires. Avoir des connaissances équivalentes ou avoir suivi la formation Cloud 360°.

Public

| Tous publics et métiers intéressés par la sécurité dans le cloud, dont les équipes techniques (développeurs, ingénieurs, architectes, devops,...), les décideurs (CTO, CISO, CxO).

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

le 7 mai 2024
le 4 juin 2024
le 9 juillet 2024
le 13 août 2024
le 24 septembre 2024
le 15 octobre 2024
le 19 novembre 2024
le 17 décembre 2024

VOIR TOUTES LES DATES

Programme de la formation

Introduction à la sécurité du cloud computing
| Les principes fondamentaux de la sécurité sur le cloud
| Les modèles de déploiement cloud (IaaS, PaaS et SaaS) et le principe de responsabilité partagée.
| Les principales menaces sur le cloud avec des exemples d'incidents réels.

Gestion des identités et contrôle d'accès
| Le rôle de l'IAM dans la protection des environnements cloud.
| Principales attaques contres l'IAM
| Bonnes pratiques pour se protéger contre le vol d'identités cloud et contre les abus de contrôle d'accès.

Sécurité des services IaaS et PaaS
| Les risques liés au IaaS et au PaaS.
| Limitation de la surface d'attaque sur les machines virtuelles et automatisation du hardening et du patching.
| Confidential Computing
| Segmentations et Isolation : les différents mécanismes.

Sécurité de la donnée
| Les risques liés au « Cloud Storage ».
| Chiffrement des données en transit et au repos.
| Prévention de la fuite de données.

| Stratégies de protection contre les ransomwares
| Identification des données sensibles grâce aux outils DLP (Data Loss Protection).

Sécurité des applications
| Emploi des outils de sécurité pour les applications déployées sur le cloud.
| Protéger les applications sur les cloud à l'aide d'outils fournis par les cloud providers : Firewall applicatifs (WAF), solutions anti-DDoS, etc.
| Bonnes pratiques sur la sécurité des applications sur le cloud.

Le SecOps sur le cloud
| Détection des événements de sécurité à l'aide des fonctions de logging et intégration avec les outils SIEM.
| Les solutions de sécurité mises à disposition par les cloud providers.
| Les solutions tierce-partie de maintien de la posture de sécurité cloud (CSPM).

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785