Formation Cloud Computing, sécurité

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

Comment peut-on assurer la sécurité des informations dispersées dans "le nuage" ? Ce séminaire dresse un panorama complet de ce problème majeur du Cloud. A l'issue, les participants auront acquis les connaissances essentielles permettant de se présenter au passage de la certification CCSK de la Cloud Security Alliance.

Référence	OUD
Durée	2 jours (14h)
Tarif	1 990 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 18 au 19 juin 2024
du 3 au 4 octobre 2024
du 14 au 15 novembre 2024

PARIS

du 11 au 12 juin 2024
du 26 au 27 septembre 2024
du 7 au 8 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Découvrir les bases du Cloud, ses différents modes de déploiement
| Évaluer les principales menaces et vulnérabilités du Cloud
| Acquérir les principes clés du référentiel Security Guidance for Critical Areas of Focus in Cloud Computing
| Identifier les trente-cinq risques identifiés par l'ENISA
| Découvrir les principes d'audit de la sécurité dans le Cloud

Public

| DSI,
| RSSI,
| responsables sécurité,
| chefs de projets,
| consultants, administrateurs.

Prérequis

| Des connaissances de base sur l'informatique sont nécessaires.

Programme de la formation

Introduction à la sécurité du Cloud Computing
| Définition du Cloud Computing (NIST, Burton Group).
| Les principaux fournisseurs et les principales défaillances déjà constatées.
| SecaaS (Security as a Service).
| Les clés d'une architecture sécurisée dans le Cloud.
| La sécurité des environnements virtuels
| Les apports de la virtualisation pour la sécurité.
| Menaces et vulnérabilités spécifiques.
| Trois modèles d'intégration de la sécurité : Virtual DataCenter, Appliance matérielle et Appliance virtuelle.
| Les solutions de sécurité dédiées à la virtualisation.

La sécurité des accès réseaux au Cloud
| Vulnérabilités et enjeux de la sécurité d'accès.
| La sécurité native dans IP v4, IPsec et IP v6.
| Les protocoles : PPTP, L2TP, IPsec et VPN SSL.
| L'accès au Cloud via le Web sécurisé (https).
| Les vulnérabilités des clients du Cloud (PC, tablettes, smartphones) et des navigateurs.

Les travaux de la Cloud Security Alliance (CSA)
| Le référentiel Security Guidance for Critical Areas of Focus in Cloud Computing.
| Les treize domaines de sécurité. Les sept principales menaces.
| La suite intégrée GRC.

| CloudAudit, Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire, Cloud Trust Protocol.
| La certification CCSK (Certificate of Cloud Security Knowledge).

La sécurité du Cloud Computing selon l'ENISA
| Evaluation et gestion des risques du Cloud par la norme ISO 27005.
| Les trente-cinq risques identifiés par l'ENISA. Les recommandations ENISA pour la sécurité des Clouds gouvernementaux.

Les recommandations du NIST pour la sécurité
| Les lignes directrices pour la sécurité et la confidentialité dans le Cloud Computing public.
| Analyse des standards NIST 800-144 et NIST 800-146.

Contrôler la sécurité du Cloud
| Quel label de sécurité pour les fournisseurs : Cobit, ISO2700x, critères communs ISO 15401 ?
| Comment auditer la sécurité dans le Cloud ?
| Les outils de contrôle de sécurité orientés Cloud (Metasploit & VASTO, openVAS, xStorm, etc.).

Aspects juridiques
| Du Cloud privé au Cloud public : conséquences juridiques. Responsabilités des différents acteurs.
| La conformité réglementaire (PCI-DSS, CNIL, SOX...).
| Les précautions pour la rédaction d'un contrat.

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.