Formation Sécurité du Cloud Computing

Synthèse de la sécurité du Cloud et des nouveaux usages des technologies

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

Présenté comme un moyen de réduire les coûts et de simplifier la gestion des moyens, le Cloud redessine les usages de l'informatique. Le positionner dans un contexte opérationnel comme la mobilité des employés et l'accès aux ressources informatiques en tout lieu, à tout moment et avec tout type de terminaux, nous permet de mesurer la complexité de son déploiement. Quelle que soit sa nature, privée ou publique, l'adoption du cloud doit s'accompagner de réflexions approfondies sur la sécurité. Ce séminaire s'appuie sur les travaux d'organismes de standardisation et sur un panorama des solutions du marché pour présenter la sécurité du Cloud dans un contexte opérationnel.

Référence	RES236
Durée	2 jours (14h)
Tarif	1 990 €HT

Objectifs

| Identifier comment s'appuyer sur des référentiels de normes et de standards pour sécuriser le Cloud
| Identifier les moyens génériques de la sécurité du Cloud
| s'inspirer des solutions et des démarches des opérateurs de Cloud pour sécuriser son approche
| Identifier comment éviter la mise en place d'une sécurité coûteuse et laborieuse pouvant dégrader la performance du réseau global

Public

| Directeurs du système d'information ou responsables du service informatique souhaitant analyser les risques liés à l'utilisation d'une solution Cloud
| Responsables et chefs de projet en charge de la mise en place d'une politique de sécurité lié à un proje

Prérequis

| Ce séminaire nécessite une connaissance sommaire de l'informatique

Programme de la formation

Introduction
| Rappel des éléments matériels et logiciels de l'architecture Cloud selon les organismes de standardisation NIST (National Institute of Standards and Technology)
| Complexité du contexte de l'utilisation en tout lieu avec tout type de terminaux de connexion

Déceler les points de vulnérabilité du Cloud
| Solutions et architectures du Cloud proposées par des grands acteurs du secteur (OS Cloud, virtualisation, stockage, Datacenter, réseaux...)
| Points de vulnérabilité du terminal d'accès au Datacenter du Cloud
| Problèmes de sécurité spécifique aux Clouds ouverts et interconnectés
| Quatre niveaux de sécurité (technologique, organisationnel, contractuel et de conception d'architectures techniques)

S'inspirer des recommandations d'organismes officiels CSA (Cloud Security Alliance) et ENISA (European Network and Information Security Agency) pour

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 12 au 13 juin 2025
du 28 au 29 août 2025

PARIS
du 12 au 13 juin 2025
du 28 au 29 août 2025

AIX-EN-PROVENCE
du 28 au 29 août 2025
du 27 au 28 novembre 2025

BORDEAUX
du 12 au 13 juin 2025
du 27 au 28 novembre 2025

GRENOBLE
du 12 au 13 juin 2025
du 27 au 28 novembre 2025

LILLE
du 12 au 13 juin 2025
du 27 au 28 novembre 2025

LYON
du 12 au 13 juin 2025
du 27 au 28 novembre 2025

NANTES
du 28 au 29 août 2025
du 27 au 28 novembre 2025

VOIR TOUTES LES DATES

sécuriser le Cloud et gérer les risques
| Protection d'accès à distance au Cloud et Datacenter (firewall multifonctions)
| Sécurité des transactions en ligne par la cryptologie (PKI)
| Authentification des accès : NAC, RBAC, portail captif, authentification forte
| IAM (Identity and Access Management)
| Surveillance des activités anormales (IDS/IPS, NIDS/NIPS)
| SIEM (Security Information and Event Management)
| Lutte contre le vol de données (DLP : Data Lost Prevention)
| 35 types de risques selon ENISA
| Traitement des 5 risques majeurs et fréquents en s'appuyant sur les recommandations d''ENISA

S'appuyer sur les solutions techniques de sécurité du Cloud, proposées par les constructeurs et opérateurs Cloud
| Synthèse des approches, matériels et logiciels de sécurité adoptés par des fournisseurs de Cloud
| Solutions de sécurité offertes par les opérateurs de Cloud public
| Internalisation des dispositifs privés dans le Datacenter du Cloud
| Cloud intermédiaire de sécurité (SecaaS : Security as a Service)
| Avantages et inconvénients de chaque solution

Sécuriser le Cloud par l'organisation des processus et le contrat de SLA
| Classification des applications éligibles pour le Cloud
| Évaluation des risques et mise en place de leur gestion
| Plan de reprise d'activité
| Choix entre les Clouds souverains et ouverts
| Définir les critères de SLA de sécurité
| Responsabilité de l'entreprise : terminaux d'accès et réseaux locaux et distants
| Responsabilités partagées des parties prenantes (entreprise cliente et son fournisseur des services du Cloud) en cas de problèmes liés à la sécurité

Sécuriser le Cloud par la conception des architectures
| Isolement et étanchéité des solutions impliquées (Virtualisation, Stockage, orchestration, API, connecteurs...) et des applications
| Association des moyens de protection, en fonction du niveau de sécurité nécessaire des éléments du Cloud
| Cloud hybride
| Cryptage de la transmission au niveau des réseaux locaux du Datacenter
| Firewall local au sein du Cloud
| Sécuriser les accès locaux et distants au Cloud en tout lieu pour des terminaux mobiles : VPN SSL, VPN IPSec et IEEE802.11i
| Dispositifs out-band de sécurité et de Firewall d'identité pour les accès mobiles en local
| Impact des solutions incohérentes de sécurité et métriques de qualité indispensable
| Ingénierie du trafic IP et des flux de données pour le bon fonctionnement des applications

Sécuriser l'utilisation des périphériques personnels des employés pour accéder au Cloud (BYOD : Bring Your Own Device)
| Choix des solutions sécurisées d'accueil des terminaux (VDI, TS-WEB, RDP, PCoIP...)
| Sélection des périphériques : tablettes, Smartphone, OS, navigateurs.... et leurs contraintes
| Étude des vulnérabilités pour fixer les règles d'utilisation d'accès au Cloud
| Affectation des droits selon des critères techniques et organisationnels

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.