


Cybersécurité & Cloud computing

Mise en œuvre des bonnes pratiques de sécurisation dans un environnement informatique en nuage.

 Cours en présentiel ou distanciel

 Durée : 2 jours (14h)



La transformation numérique des systèmes d'information est un enjeu de développement majeur pour les entreprises et les organisations. Le Cloud est l'un des outils technologiques indispensables pour atteindre cet objectif. Mais les risques qui pèsent sur les données des entreprises se sont considérablement accrus. En effet, les données de l'entreprise sont désormais hébergées chez des fournisseurs de services Cloud et ces derniers sont des cibles de choix pour des cybercriminels qui cherchent l'opportunité de s'approprier de grandes quantités d'informations. Ce cours technique permettra aux participants d'identifier les menaces émergentes qui pèsent sur les données de l'entreprise et de comprendre quelles évolutions techniques et organisationnelles peuvent permettre de s'en prémunir.

Les objectifs de la formation

L'objectif de cette formation est d'aborder les différentes problématiques et solutions de la sécurisation du Cloud :

- Comprendre les enjeux de la cybersécurité.
- Connaître les bonnes pratiques ainsi que les normes et standards pour sécuriser le Cloud.
- Savoir mettre en œuvre la sécurisation des données personnelles et la conformité réglementaire dans le Cloud.
- Savoir mettre en œuvre une gouvernance efficace et une politique de sécurité maîtrisée.
- Connaître l'étendue des risques qui pèsent sur les données numériques de votre entreprise.
- Identifier les risques liés à l'émergence des nouvelles technologies.
- Savoir utiliser les services proposés par les fournisseurs Cloud pour sécuriser une infrastructure virtualisée.
- Connaître les différents outils disponibles en ligne pour se prémunir des infections.
- Comprendre l'intérêt de disposer d'une surveillance et d'une gestion des incidents.

Pour qui ?

Personnes concernées :

- Toute personne en charge de la sécurité d'un système d'information : administrateur système/réseau, directeur des services informatiques (DSI), responsable de sécurité des systèmes d'information (RSSI)
- Consultants, experts et auditeurs en sécurité
- Enseignants, chercheurs et étudiants en sécurité informatique

Prérequis :

- Connaissances basiques en informatique : fonctionnement des systèmes d'information, des réseaux, des systèmes d'exploitation et des applications.
- Connaissances des bases de la sécurité informatique

Prérequis techniques

Pour les formations en distanciel, il est impératif d'avoir un ordinateur équipé d'une carte son et idéalement posséder un casque avec micro intégré. La Webcam est un plus mais n'est pas obligatoire.

Méthode et Moyens pédagogiques

- Cette formation alterne les exposés théoriques et les travaux pratiques : 60 % d'apports théoriques et 40 % d'exercices pratiques.
- Méthode active à travers l'articulation de situations d'apprentissage et de techniques pédagogiques multiples.

Evaluation des connaissances et suivi de l'exécution de la prestation

- Un questionnaire est envoyé en amont de la formation pour recueillir les attentes des stagiaires et adapter la formation au plus près des attentes de chacun
- Un questionnaire d'évaluation des acquis de la formation est soumis en fin de formation ainsi qu'un questionnaire de satisfaction
- Un Support pédagogique et une attestation de formation est fournie à chaque stagiaire en fin de la formation.

Programme de la formation

Introduction à la sécurité du Cloud

Concepts fondamentaux du Cloud

- Définition, description et analogie
- Les modèles de déploiement (public, privé, hybride, communautaire, multcloud)
- Les modèles de service (IaaS, SaaS, PaaS)
- Les nouveaux modèles de services cloud (XaaS/EaaS : STaaS, DaaS, DBaaS, FaaS, BaaS, DRaaS, etc.)

- Architecture du Cloud Computing (NIST, ISO 17788/17889)
- Les principales technologies impliquées dans les *datacenters* (virtualisation, *Grid Computing*, stockage et distribution de contenu, etc.)
- Les principaux fournisseurs (AWS, Azure, Google Cloud, etc.)
- Les solutions proposées (service, stockage, outils collaboratifs, etc.)
- Exemples concrets d'utilisation
- Les avantages du cloud computing
- Les inconvénients du cloud computing

Problématiques de la sécurité du Cloud

- Sécurité « On-Premise » VS dans le Cloud
- Évaluer les principales menaces, vulnérabilités et risques dans le Cloud
- Les risques identifiés par l'ENISA (agence de l'Union européenne pour la cybersécurité)
- Evaluation et gestion des risques du Cloud par la norme ISO 27005

Standards de sécurité du Cloud

Principes et règlements

- Le principe de responsabilité partagée dans les modèles de service du Cloud
- Les référentiels de la Cloud Security Alliance (CSA)
- La sécurité dans les contrats Cloud
- Les réglementations et aspects juridiques : les lois et dispositions européennes (RGPD) et américaines (Privacy Shield, Patriot Act., FISA, Cloud Act)

Normes et techniques de sécurité des données

- Les normes ISO 27017 et 27018 pour sécuriser les données dans le cloud
- La cryptographie dans le Cloud
 - Les fondamentaux (cryptographie, cryptanalyse, etc.).
 - Les approches de gestion des clés de chiffrement dans le Cloud.
 - Les approches BYOK (Bring Your Own Key) et KSaaS (Key Storage as a Service).
 - Les solutions hardware des clés (cartes et appliances HSM).
- Autres techniques de protection des données

Assurer la sécurité du cloud

- La stratégie de sauvegarde et de back-ups
- Les outils de sauvegarde tiers (Veeam, etc.)
- Meilleures pratiques pour la sécurité du Cloud
- Les 7 risques de sécurité du cloud computing
- Les 10 principales recommandations de la liste de contrôle de sécurité pour les clients du Cloud

- Certifications de sécurité ISO 27001 ou SSAE16 type II (SAS 70) de fournisseurs Cloud
- Cloud Access Security Broker (CASB)
- Schémas d'audit de la sécurité du Cloud.
- Audits de contrôle de sécurité orientés Cloud (Metasploit, etc.)
- Scans de sécurité (Nessus, Alert Logic, Symantec o3, Qualys, etc.)
- Détection d'intrusions

Cas Pratique appliqué au Cloud Azure

Gestion des identités et droits utilisateurs

- Gestions des identités
 - Utilisation d'Azure Active Directory
 - Ajout d'un utilisateur manuellement
 - Mise en place des groupes dans Azure AD
 - Mise en place authentification forte
 - Jonction d'un poste Windows 10 à Azure AD
- Droits utilisateurs sur les applications/services
 - Azure AD et les applications
 - Ajout d'une application dans le portail
 - Mise en place d'un accès conditionnel

Cas pratique - Approche "Security by design" dans le Cloud Amazon

Principe du "Security by design"

- Stratégies de sécurisation du Cloud Amazon
- Le principe du "Security by design"
- La gouvernance des comptes sur AWS

Archivage Electronique Sécurisé

- Création d'une identité
- Utilisation de la traçabilité
- Protection des données