Sécuriser ses infrastructures Cloud : Les fondamentaux

Comprendre et mettre en oeuvre la sécurité dans le Cloud

3 jours / 21 heures | **Valence** | **Ref : CLOUD1**

PRÉSENTATION

Ces dernières années ont été le témoin de l'essor de cyber-incidents affectant, à divers degrés, tout un chacun. Qu'il s'agisse d'incivilité, de harcèlement, d'escroquerie, de fraude, de vol, de destruction, de dysfonctionnement, de surveillance, d'espionnage, d'activisme ou encore par exemple de terrorisme ou de désinformation, toute forme de délit, de violence ou de conflictualité se matérialise via l'Internet. Les infrastructures Cloud sont donc particulièrement exposées, et la cible d'attaques de plus en plus fréquentes. C'est pourquoi il convient de comprendre quelles sont les mesures à mettre en œuvre afin de déployer une solution de Cloud Computing performante et sécurisée, sans risquer de compromettre son système d'information.

—TEST D'INTRUSION

—CYBERSÉCURITÉ

—HACKING

OBJECTIFS DE LA FORMATION

OBTENIR une vision globale des offres de Cloud Computing et des fournisseurs
COMPRENDRE les risques induits par ces services en termes de sécurité de l'information
AVOIR une vision globale des aspects de conformité (juridique, niveaux de service, audit, standards, etc.)
COMPRENDRE la sécurité d'une architecture de Cloud Computing
SAVOIR répondre à un incident de sécurité

PUBLIC VISÉ

Consultants en sécurité
Techniciens
Administrateurs systèmes / réseaux
Développeurs

PRÉREQUIS

Aucun prérequis spécifique

POUR ALLER PLUS LOIN..

Sensibilisation à la Cybersécurité : [Ref : SENSI1]
Cybersécurité : Les fondamentaux [Ref : SECU1]

LES + DE LA FORMATION

DES EXPERTS

du Cloud Computing pour vous former

DES BONNES PRATIQUES

en matière de sécurité dans le Cloud Computing regroupées dans un référentiel exhaustif

DES COMPÉTENCES

immédiatement applicables et valorisables pour tout projet ou solution Cloud actuelle ou future

Programme

JOUR 1

Introduction à la sécurité du Cloud Computing

- Vocabulaire et terminologie
- Définitions du Cloud (NIST, IBM, CISCO, etc.)
- Panorama des offres de services et des principaux fournisseurs
- État du niveau de service et défaillances déjà constatées
- Les clés d'une architecture sécurisée

JOUR 2

Sécurité des plateformes de Cloud

- Point sur les technologies employées : points forts et avantages
- Menaces et vulnérabilités spécifiques
- Solutions de sécurité en oeuvre chez les principaux fournisseurs
- Conception de solutions sur-mesure

Sécurité des accès réseaux au Cloud

- Vulnérabilités et enjeux de la sécurité d'accès
- La sécurité native dans IPv4, IPsec et IPv6
- 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

JOUR 3

Contrôler la sécurité du Cloud

- Panorama des labels de sécurité pour les fournisseurs : COBIT, ISO, 27001, 27002, 27005
- Méthodologie d'audit de sécurité dans le Cloud
- Outils de contrôle de l'exposition et de la sécurité appliqués au Cloud Computing

Aspects juridiques et contractuels du Cloud

- Du Cloud privé au Cloud public : conséquences juridiques et responsabilités des différents acteurs
- La conformité réglementaire : RGPD, CNIL, ISO22301, etc.
- Contractuellement, que proposent les principaux fournisseurs de services ?
- Qu'est-ce qu'un bon contrat de Cloud Computing ?

Grenoble INP ESISAR
ÉCOLE NATIONALE SUPÉRIEURE EN SYSTÈMES AVANCÉS ET RÉSEAUX
Contact : numericlab@esynov.fr | Site internet : www.esynov.fr
NANOELEC.