

Formation Cloud Computing - Sécurité

Informations

Durée : 3 jours (21h.)

Tarif* : Nous consulter

Réf : CLOS

Niveau : Difficile

intra

*tarif valable jusqu'au 31/12/2024

Prochaines sessions

Contactez-nous pour connaître nos futures sessions.

Pré-requis

- Avoir des connaissances sur le Cloud Computing ou avoir suivi la formation Cloud Computing - Synthèse Pratique (CLOP)

Objectifs

- Analyser, gérer et implémenter la sécurité pour des architectures clouds publiques et privées
- Mettre en place le respect de la vie privée et vérifier l'intégrité des données sur le cloud
- Garantir la sécurité des applications lors de l'utilisation d'un PaaS

Programme

Rappels sur le Cloud computing

Définition du cloud computing : SaaS, PaaS, IaaS / cloud privé, cloud public

Les promesses du cloud computing

Panorama des acteurs et des offres existantes

Normes en cours de développement

Synthèse des bonnes pratiques de gouvernance (contrat, SLA, confidentialité, sécurité, réversibilité) et d'architecture (architecture interne, cloud, hybride, intégration)

Sécurisé un Cloud

Analyses de sécurité : opportunité et contraintes, évaluation de la sécurité, critères de choix

Conformité : aspects légaux et contractuels, niveaux de services, audits, standards et certifications

Architecture : sécurité des données, sécurité des systèmes et des applications, gestion des identités et des accès, gestion de la cryptographie, virtualisation

Réaction aux incidents de sécurité

La sécurité de la virtualisation

Les risques liés à la virtualisation des serveurs

Quelles sont les technologies de virtualisation déployées dans les principales offres de Cloud public ?

Les avantages de la virtualisation pour la sécurisation du SI

Panorama des menaces et vulnérabilités spécifiques à la virtualisation

Les six risques majeurs identifiés par le Gartner : comment les gérer ?

Attaques sur les machines virtuelles (VM Escape, VM Hopping, VM Theft et VM Sprawl).

Hyperkit et hyperjacking : mythe ou réalité ?

Protection des environnements virtuels

Utilisation de la virtualisation pour accroître la sécurité du SI

L'approche sécurité de VMware : API VMsafe, partenariats et offre produit VShield Endpoint.

La gestion des incidents de sécurité dans un environnement virtualisé

Les bonnes pratiques pour la sécurité des environnements virtuels

Les recommandations de l'ANSSI, du NIST (SP 800-125) et de la Cloud Security Alliance

Pourquoi les solutions anti-malware classiques sont-elles inadaptées aux infrastructures virtualisées ?

La sécurité des accès au Cloud et des terminaux

La sécurisation des accès au Cloud

Formation Cloud Computing - Sécurité

L'apport sécurité des protocoles IPsec et IPv6

Les technologies classiques de VPN (L2TP, IPsec, VPN SSL) sont-elles adaptées au Cloud ?

Les firewalls UTM et les pare-feu applicatifs (WAF) sont-ils encore efficaces ?

Les solutions spécifiques d'accès au Cloud (Ex : CloudGate d'Intercloud)

Les solutions CASB (Cloud Access Security Broker) sont-elles simplement utiles ou indispensables ?

Panorama de l'offre CASB actuellement disponible sur le marché.

La sécurité des postes clients

Comment la consomérisation de l'IT et le BYOD impactent-ils la sécurité du Cloud ?

Smartphones et tablettes Windows, iPad et Android : quels sont les risques ?

Peut-on y remédier ?

Le navigateur Web est-il le talon d'Achille de la sécurité du Cloud ?

Les bonnes pratiques pour sécuriser les postes clients

Les principaux travaux sur la sécurité du Cloud

La sécurité du Cloud selon l'ENISA

Comment utiliser la norme ISO 27005 pour évaluer les risques dans le Cloud ?

Les trente-cinq risques identifiés par l'ENISA (risques politiques et organisationnels, risques techniques, risques juridiques et risques non spécifiques au Cloud)

Les huit risques majeurs identifiés par l'ENISA et le traitement approprié

Les recommandations de l'ENISA pour la sécurité des Clouds gouvernementaux

La sécurité du Cloud analysée par la Cloud Security Alliance (CSA)

Les neuf principales menaces identifiées dans le Cloud.

Le Framework OCF et l'annuaire STAR (Security, Trust & Assurance Registry) pour la transparence des pratiques de sécurité des fournisseurs de Cloud

Comment utiliser la Cloud Controls Matrix (CCM) et le questionnaire CAIQ ?

La certification des connaissances en sécurité du Cloud : CCSK (Certificate of Cloud Security Knowledge)

Les recommandations du NIST pour la sécurité du Cloud

Standard NIST 800-144 : lignes directrices pour la sécurité et la confidentialité dans le Cloud Computing public

L'approche française de la sécurité du Cloud

Les recommandations de l'État français (ANSSI). Le guide ANSSI : "Maîtriser les risques de l'infogérance"

Le référentiel ANSSI de qualification de prestataires de services sécurisés d'informatique en nuage

Les recommandations de la CNIL pour protéger les données à caractère personnel dans le Cloud

Le point de vue des grandes entreprises françaises et des cabinets d'audit français (CIGREF et AFAI)

Le projet de Cloud souverain (Andromède) : Numergy VS Cloudwatt