Cloud : Gouvernance et Sécurité

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Systèmes et Réseaux

Filière : Cloud computing

Rubrique : Action collectives

Éligible au CPF : Non

Action collective : Non

PRÉSENTATION

Objectifs & compétences

Comprendre les éléments fondamentaux de la sécurité du Cloud Identifier et analyser les risques liés au Cloud Comprendre les contrats Cloud Mettre en oeuvre les bonnes pratiques de sécurité dans le Cloud Connaître les techniques de sécurisation réseau du Cloud.

Public visé

Architectes, chefs de projets, ingénieurs informatique (réseau, système, développement...).

Pré-requis

Avoir des connaissances minimales sur le Cloud (caractéristiques, modèles de services, modèles de déploiement) et des bases en sécurité informatique et réseaux. Avoir également des notions de management de projet.

PROGRAMME

Introduction à la sécurité du Cloud Computing

- Définition du Cloud Computing (NIST) et norme ISO 17788.
- Les principaux fournisseurs et les principales défaillances déjà constatées.
- Les offres de SecaaS (Security as a Service).
- Les clés d'une architecture sécurisée dans le Cloud.

La sécurité des environnements virtuels

- Les risques liés à la virtualisation des serveurs (VM Escape, VM Hopping, VM Theft et VM Sprawl).
- La problématique de la protection anti-malware dans une infrastructure virtualisée.
- Les risques liés aux vulnérabilités, aux API et aux logiciels (Openstack, Docker, VmWare...).

La sécurité des accès réseaux au Cloud

- Les accès sécurisés via Ipsec, VPN, https et SSH.
- Les solutions spécifiques d'accès au Cloud (Intercloud, AWS Direct connect...).
- Les solutions CASB (Cloud Access Security Broker).
- 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 douze principales menaces identifiées dans le Cloud.
- Le framework OCF et l'annuaire STAR (Security, Trust & Assurance Registry).
- Comment utiliser la Cloud Controls Matrix (CCM) et le questionnaire CAIQ ?

Code de formation : ACF101

€ Tarifs

Prix public : 2890 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 21 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 11/11/2026

- La certification des connaissances en sécurité du Cloud : 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.

Contrôler la sécurité du Cloud

- Comment contrôler la sécurité dans le Cloud : audit, test d'intrusion, qualification, certification ?
- Que valent les labels de sécurité Secure Cloud, CSA STAR et Cloud confidence ?
- Comment opérer un contrôle continu de la sécurité pendant toute la durée du contrat ?
- Comment sont détectés et notifiés les incidents de sécurité dans le Cloud ?

Le contrat Cloud

- Les clauses de sécurité indispensables à insérer dans un contrat de Cloud (comité de suivi, confidentialité...).
- Les clauses de réversibilité (amont & val) pour ne pas se faire piéger par un fournisseur.
- La clause d'audit de sécurité : peut-on toujours la négocier ? Comment faire dans un Cloud public ?
- L'importance de la localisation des données et de la juridiction retenue.
- Les accords de service dans le Cloud (SLA).
- Pénalités et indemnités : bien comprendre les différences.

Aspects juridiques et conformité réglementaire

- Quelles sont les responsabilités juridiques du fournisseur ? Quid des sous-traitants du fournisseur ?
- La nationalité du fournisseur et la localisation des Datacenters.
- Le cadre juridique des données à caractère personnel (Directive 95/46 CE, GDPR, CCT, BCR...).
- Après l'annulation du « Safe harbor », quelles sont les nouvelles garanties apportées par le « Privacy Shield » ?
- Le point sur l'USA Patriot Act. Menace-t-il les données dans le Cloud à l'extérieur des USA ?
- Le cadre juridique des données de santé à caractère personnel (loi du 26 janvier 2016).
- Les hébergeurs de données de santé (agrément ASIP, obligations de sécurité, localisation des données, etc.).

Les normes de sécurité dans le Cloud

- Que vaut la certification de sécurité ISO 27001 affichée par les fournisseurs ?
- Les normes ISO/IEC 17788:2014 (vocabulaire) et ISO/IEC 17789:2014 (architecture de référence).
- Les nouvelles normes ISO/IEC (27017 & 27018) dédiées à la sécurité dans le Cloud.
- Quel apport de la norme ISO 27018 pour la protection des données personnelles dans le Cloud ?
- La norme ISO 27017 et son complément idéal CSA Cloud Control Matrix.

La gestion des licences dans le Cloud

- Comprendre pourquoi la gestion des licences est plus complexe dans le Cloud.
- Comment assurer la conformité ?
- Les limites des outils de gestion des actifs logiciels (Software Asset Management) dans le Cloud.
- Réaliser l'inventaire et faire le rapprochement entre les licences installées, acquises et utilisées dans le Cloud.

Informations non contractuelles - PDF généré le 11/11/2026

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 11/11/2026