Sécurité du Cloud

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : PAO et bureautique

Action collective : Non

Filière : Bureautique

Rubrique : Microsoft Access

PRÉSENTATION

Objectifs & compétences

A l'issue de la formation, le stagiaire sera capable d'engager une démarche sécurisée des projets Cloud, en adoptant une approche technique, métier et légale du sujet, adaptée au contexte opérationnel.
Connaitre les fondamentaux de la sécurité des SI et du Cloud
Appréhender les principales menaces, vulnérabilités et risques du Cloud
Connaitre les référentiels de normes et de standards pour sécuriser le Cloud
Évaluer la maturité et le niveau de sécurité des fournisseurs cloud
Identifier les aspects organisationnels de la sécurité du cloud
Identifier les bonnes pratiques et les solutions de sécurisation des opérateurs de Cloud

Public visé

DSI, RSI, Chefs de projets, Responsables sécurité, Consultants, Administrateurs, toute personne en charge de la sécurité du Cloud Computing

PROGRAMME

Module 1 : Introduction au cloud computing

- Modèles : SaaS, PaaS, IaaS
- Types : public, privé, hybride

Module 2 : Sécurité : défis dans le nuage

- Présentation du sujet – Pourquoi est-ce difficile ?
- Virtualisation et multi-location
- L'évaluation des risques pour la migration

Module 3 : La sécurité des infrastructures dans le nuage

- La gestion de patch et de configuration
- La sécurité des réseaux et la virtualisation
- La sécurité et l'impact pour les applications
- La sécurité des données

Module 4 : Les risques et la gouvernance pour le cloud computing

- La nécessité des politiques internes et des exigences
- Service Level Agreements (SLA)
- Les modèles de gouvernance pour le nuage et la gestion des risques
- La réversibilité

Module 5 : Audit et évaluation du cloud

- Audit du cloud à distance et sur place
- Les évaluations pour le nuage
- Cloud Security Alliance et A6 CloudAudit [2]

Code de formation : S-CLS

#CLOUD #ACTIONCOLLECTIVE #COMPUTING

€ Tarifs

Prix public : 1890 €

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

Campus : Ensemble des sites

Durée : 14 heures

Rythme : 2 jours. 10 et 11 Septembre 202619 et 20 Novembre 2026

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

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 03 / 07 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 14 heures
  : 2 jours

- 13 / 10 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 14 heures
  : 2 jours

Informations non contractuelles - PDF généré le 18/11/2026

- Pen-tester le nuage

Module 6 : La sécurité des données dans le cloud

- Types de chiffrement et disponibilité
- Les données et leur cycle de vie
- La gestion des clés de chiffrement

Module 7 : Gestion des Identités et des Accès (IAM)

- Architecture IAM et sa pertinence dans le "cloud"
- Normes d'authentification et d'autorisation
- La gestion des comptes, la fédération et le provisionnement

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 18/11/2026