AWS Ingénierie Sécurité

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : PAO et bureautique

Action collective : Non

Filière : Bureautique

Rubrique : Microsoft Access

Code de formation : AWS005

#CLOUD #ACTIONCOLLECTIVE #COMPUTING

PRÉSENTATION

Objectifs & compétences

A l'issue de la formation, le stagiaire sera capable d'utiliser efficacement les outils et les services de sécurité AWS pour protéger ses données et systèmes dans l'environnement Cloud d'Amazon Web Services.
–> La formation vise l'acquisition des connaissances et compétences rattachées au cours officiel d'Ingénierie de sécurité sur AWS (ou équivalent en cas d'évolution décidée par l'éditeur).
–> Ce cours s'inscrit dans le cursus de certification proposé par l'éditeur mais le passage de l'examen n'est pas compris dans la présente consultation.
Comprendre et tirer avantage du modèle de sécurité en responsabilité partagée d'AWS ?
Gérer les identités des utilisateurs et leur accès sur l'environnement AWS
Utiliser les services de sécurité AWS tels que AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM, et AWS Trusted Advisor
Implémenter de meilleurs contrôles de sécurité pour vos ressources sur AWS
Gérer et auditer vos ressources du point de vue de la sécurité
Superviser et tracer les accès et les usages des ressources AWS, telles que les instances, le stockage, le réseau et les services de bases de données
Identifier les services et les outils AWS qui permettent d'aider l'automatisation, la surveillance et la gestion des opérations de sécurité sur AWS
Gérer les incidents de sécurité sur l'environnement AWS

Public visé

Ingénieurs sécurité, Architectes sécurité, Auditeurs en sécurité, toute personne en charge de la sécurité de l'information…

Pré-requis

Avoir des connaissances des pratiques de sécurité dans le domaine de l'informatique en général. Avoir de l'expérience en gouvernance, contrôle, évaluation du risque et de conformité aux normes. Il est recommandé d'avoir suivi le cours « AWS Architecture ».

PROGRAMME

Module 1 : Sécurité AWS

- Principes de conception de la sécurité dans le cloud AWS
- Modèle de responsabilité partagée AWS
- DevOps avec ingénierie de la sécurité

Module 2 : Identifier les points d'entrée sur AWS

- Bonnes pratiques sur les informations d'identification de l'utilisateur
- Analyse des politiques IAM
- Authentification multifacteur
- AWS CloudTrail

Travaux pratique :

€ Tarifs

Prix public : 2395 €

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 : 21 heures

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 :

- 22 / 09 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 21 heures
  : 3 jours

- 15 / 12 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 21 heures
  : 3 jours

Authentification entre comptes

Module 3 : Sécurité des environnements Web applicatifs

- Menaces dans une architecture à trois niveaux
- AWS Trusted Advisor

Module 4 : Sécurité des applications

- Considérations de sécurité Amazon EC2
- Inspecteur Amazon
- Gestionnaire de systèmes AWS

Travaux pratique :
Utilisation d'AWS Systems Manager et d'Amazon Inspector

Module 5 : Sécurité des données

- Protéger les données au repos avec Amazon S3
- Considérations de sécurité Amazon RDS et Amazon DynamoDB
- Protéger les données d'archives

Module 6 : Sécurisation des communications réseau

- Considérations sur la sécurité d'Amazon VPC
- Considérations sur la sécurité d'Amazon Elastic Load Balancing
- Gestionnaire de certificats AWS

Module 7 : Surveillance et collecte de journaux sur AWS

- Configuration AWS
- Amazon CloudWatch
- Amazon Macie
- Collecte de journaux sur AWS

Travaux pratique :
Surveiller et répondre avec AWS Config

Module 8 : Traitement des journaux sur AWS

- Amazon Kinesis
- Amazon Athena

Travaux pratique :
Analyse des journaux de serveur Web avec Amazon Kinesis et Amazon Athena

Module 9 : Considérations de sécurité : Environnements hybrides

- AWS VPN connections
- AWS Direct Connect
- AWS Transit Gateway

Module 10 : Protection hors région

- Amazon Route 53
- Amazon CloudFront
- AWS WAF
- AWS Shield
- AWS Firewall Manager

Module 11 : Sécurisation des environnements Serverless

- Amazon Cognito
- Amazon API Gateway
- AWS Lambda

Module 12 : Détection des menaces et enquête

- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective

Module 13 : Gestion des secrets sur AWS

- AWS KMS

- AWS CloudHSM
- AWS Secrets Manager

Travaux pratique :
Using AWS KMS

Module 14 : Automatisation de la sécurité sur AWS

- AWS Security by Design approach
- AWS CloudFormation
- AWS Service Catalog

Travaux pratique :
Using AWS Service Catalog

Module 15 : Gestion de compte et provisionnement sur AWS

- AWS Organizations
- AWS Control Tower
- Federated user access

Travaux pratique :
AWS Federated Authentication

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.