

Amazon Web Services (AWS) - Ingénierie de sécurité sur AWS

Cours officiel, Security Engineering on AWS

Cours Pratique de 3 jours - 21h

Réf : AWJ - Prix 2024 : 2 480€ HT

Le prix pour les dates de sessions 2025 pourra être révisé

Avec cette formation, vous apprenez à utiliser de manière efficace les services sécurité AWS pour garantir la sécurité et le respect des réglementations dans le cloud AWS. Nous nous focaliserons sur les best practices sécurité que vous pouvez mettre en place pour améliorer la sécurité de vos données et systèmes.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre et tirer avantage du modèle de sécurité en responsabilité partagée d'AWS

Architecturer et construire des infrastructures d'application protégées contre les menaces communes

Protéger la donnée "à la cible" et "en transit" avec le chiffrement

Appliquer les checks et analyses de sécurité de façon reproductible et automatisé

Configurer l'authentification pour les ressources et applications dans AWS

Profiter des événements par la capture, la surveillance et l'analyse des logs

Identifier et mitiger les menaces pour les applications et la donnée

Évaluer la sécurité pour veiller à l'application des pratiques de sécurité et du patching contre les vulnérabilités

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, etc.

Gérer et auditer vos ressources du point de vue de la sécurité.

Implémenter de meilleurs contrôles de sécurité pour vos ressources sur AWS

Superviser et tracer les accès et les usages des ressources AWS

Identifier services et outils AWS qui permettent d'aider l'automatisation, la surveillance, opérations de sécurité...

Gérer les incidents de sécurité sur l'environnement AWS

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel en anglais et au format numérique. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

La réussite de l'examen permet d'obtenir la certification AWS Certified Security - Specialty. (Prérequis - avoir suivi les formations : AWS Technical Essentials ou AWS Security Essentials, Architecting on AWS et Security Engineering on AWS).

FINANCEMENT

Ce cours fait partie des actions collectives Atlas.

PARTICIPANTS

Ingénieurs sécurité, architectes sécurité, auditeurs en sécurité, toute personne en charge de la sécurité de l'information.

PRÉREQUIS

Avoir suivi la formation "Technical essentials" ou "Architecting on AWS". Connaissance des pratiques et des concepts d'infrastructure de la sécurité IT. Connaissances des concepts de cloud computing.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.

Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.

Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...

À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 01/2024

1) Sécurité sur AWS

- Sécurité dans le cloud AWS.
- Modèle de responsabilité partagée AWS.
- Présentation de la réponse aux incidents.
- DevOps avec l'ingénierie de sécurité.

2) Identification des points d'entrée sur AWS

- Identifier les différents moyens d'accéder à la plateforme AWS.
- Comprendre les stratégies IAM.
- IAM Permissions Boundary.
- IAM Access Analyzer.
- Authentification multi-facteur.
- AWS CloudTrail.

Travaux pratiques : Accès entre comptes.

3) Considérations relatives à la sécurité

- Menaces dans une architecture "trois-tiers".
- Menaces courantes : accès utilisateur.
- Menaces courantes : accès aux données.
- AWS Trusted Advisor.

4) Sécurité des applications

- Amazon Machine Images.
- Amazon Inspector.
- AWS Systems Manager.

Travaux pratiques : Utilisation d'AWS Systems Manager et d'Amazon Inspector.

5) Sécurité des données

- Stratégies de protection des données.
- Chiffrement sur AWS.
- Protecting data at rest avec Amazon S3, Amazon RDS, Amazon DynamoDB.
- Protection des données archivées avec Amazon S3 Glacier.
- Amazon S3 Access Analyzer.
- Amazon S3 Access Points.

6) Sécurité des communications réseaux

- Amazon VPC security considerations.
- Amazon VPC Traffic Mirroring.
- Réponse aux instances compromises.
- Elastic Load Balancing.
- AWS Certificate Manager.

7) Surveillance et collecte des logs sur AWS

- Amazon CloudWatch and CloudWatch Logs.
- AWS Config.
- Amazon Macie.
- Amazon VPC Flow Logs.
- Amazon S3 Server Access Logs.

- ELB Access Logs.

Travaux pratiques : Surveiller et répondre avec AWS Config.

8) Traitement des Logs sur AWS

- Amazon Kinesis.
- Amazon Athéna.

Travaux pratiques : Analyse des logs du Web Server.

9) Sécurité des environnements hybrides

- AWS Site-to-Site et Client VPN connections.
- AWS Direct Connect.
- AWS Transit Gateway.

10) Protection hors région

- Amazon Route 53.
- AWS WAF.
- Amazon CloudFront.
- AWS Shield.
- AWS Firewall Manager.
- DDoS mitigation on AWS.

11) Sécurité des environnements Serverless

- Amazon Cognito.
- Amazon API Gateway.
- AWS Lambda.

12) Détection et analyse des menaces

- Amazon GuardDuty.
- AWS Security Hub.
- Amazon Detective.

13) Secrets Management on AWS

- AWS KMS.
- AWS CloudHSM.
- AWS Secrets Manager.

Travaux pratiques : Utilisation d'AWS KMS.

14) Automatisation et sécurité dès la conception

- AWS CloudFormation.
- AWS Service Catalog.

Travaux pratiques : Automatisation de la sécurité sur AWS avec AWS Service Catalog

15) Account Management et Provisioning sur AWS

- AWS Organizations.
- AWS Control Tower.
- AWS SSO.
- AWS Directory Service.

Travaux pratiques : Federated Access avec ADFS.

LES DATES

CLASSE À DISTANCE

2024 : 16 déc.

2025 : 04 févr., 07 avr., 02 juin

PARIS

2025 : 21 janv., 03 mars, 19 mai,
01 juil.