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

Cours officiel, Security Engineering on AWS

Cours pratique - 3j - 21h00 - Réf. AWJ
Prix : 2570 € H.T.

4,4 / 5

ActionCo | Nouvelle édition

Formation éligible au financement Atlas

Avec cette formation, vous découvrirez les enjeux de sécurité pour les utilisateurs du cloud et ceux envisageant son adoption. Face à la montée des cyberattaques et des fuites de données, ce cours Security Engineering on AWS vous permettra de comprendre comment travailler de manière sécurisée avec AWS. Vous apprendrez à gérer les identités, les rôles et les comptes, à surveiller l'activité des API, à protéger les données sur AWS, et à analyser les journaux pour détecter et enquêter sur les incidents de sécurité.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Expliquer la sécurité du cloud AWS en s'appuyant sur le modèle CIA
- Créer et analyser des authentifications et des autorisations avec IAM
- Gérer et approvisionner des comptes sur AWS avec les services AWS appropriés
- Identifier comment gérer les secrets à l'aide des services AWS
- Surveiller les informations sensibles et protéger les données via le cryptage et les contrôles d'accès
- Identifier les services AWS qui répondent aux attaques provenant de sources externes
- Surveiller, générer et collecter les logs
- Identifier les indicateurs d'incidents de sécurité
- Identifier comment enquêter sur les menaces et les atténuer à l'aide des services AWS

Public concerné

Ingénieurs sécurité, architectes sécurité, architectes cloud, opérateurs cloud.

PARTICIPANTS

Ingénieurs sécurité, architectes sécurité, architectes cloud, opérateurs cloud.

PRÉREQUIS

Avoir suivi les formations AWS “Security Essential” ou "Security Fundamentals" ou “Architecting on AWS”. Connaissance des pratiques et des concepts d’infrastructure de la sécurité IT.

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 formation, 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.

Prérequis

Avoir suivi les formations AWS “Security Essential” ou "Security Fundamentals" ou “Architecting on AWS”. Connaissance des pratiques et des concepts d’infrastructure de la sécurité IT.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

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.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

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.

Programme de la formation

1 Sécurité sur AWS

- Expliquer la sécurité dans le cloud AWS.
- Expliquer AWS Shared Responsibility Model.
- Résumer IAM, la protection des données, la détection et réponse aux menaces.
- Indiquer les différentes manières d'interagir avec AWS en utilisant la console, le CLI et les SDK.
- Décrire comment utiliser l'authentification multi-facteurs (MFA) pour une protection supplémentaire.
- Indiquer comment protéger le compte utilisateur root et l'accès.

2 Sécuriser les points d'entrée sur AWS

- Décrire comment utiliser l'authentification multi-facteurs (MFA) pour une protection supplémentaire.
- Décrire comment protéger le compte utilisateur root et les clés d'accès.
- Décrire les politiques IAM, les rôles, les composants de politiques et les limites de permissions.
- Sécuriser les points d'entrée sur AWS : MFA, protection du compte root, clés d'accès et gestion des politiques IAM.
- Utiliser AWS CloudTrail pour enregistrer et consulter les demandes API, et analyser l'historique des accès.

Travaux pratiques

Utilisation des politiques basées sur l'identité et les ressources.

3 Gestion des comptes et provisionnement sur AWS

- Expliquer comment gérer plusieurs comptes AWS en utilisant AWS Organizations et AWS Control Tower.
- Expliquer comment mettre en place des environnements multi-comptes avec AWS Control Tower.
- Démontrer la capacité à utiliser des fournisseurs d'identité et des courtiers pour accéder aux services AWS..
- Expliquer l'utilisation d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) et d'AWS Directory Service.
- Démontrer la capacité à gérer l'accès des utilisateurs de domaine avec Directory Service et IAM Identity Center.

Travaux pratiques
Gestion de l'accès des utilisateurs de domaine avec AWS Directory Service.

4 Gestion des secrets sur AWS

- Décrire et énumérer les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager.
- Démontrer comment créer une clé AWS KMS multi-régions.
- Démontrer comment chiffrer un secret de Secrets Manager avec une clé AWS KMS.
- Utiliser un secret chiffré pour se connecter à une base de données Amazon RDS dans plusieurs régions AWS.

Travaux pratiques
Utilisation d'AWS KMS pour chiffrer les secrets dans Secrets Manager.

5 Sécurité des données

- Surveiller les données pour détecter des informations sensibles avec Amazon Macie.
- Expliquer comment protéger les données au repos grâce au chiffrement et aux contrôles d'accès.
- Identifier les services AWS utilisés pour répliquer les données à des fins de protection.
- Déterminer comment protéger les données une fois archivées.

Travaux pratiques
Sécurité des données dans Amazon S3.

6 Protection de l'infrastructure Edge

- Décrire les fonctionnalités AWS utilisées pour construire une infrastructure sécurisée.
- Décrire les services AWS utilisés pour créer de la résilience lors d'une attaque.
- Identifier les services AWS utilisés pour protéger les charges de travail contre les menaces externes.
- Comparer les fonctionnalités d'AWS Shield et d'AWS Shield Advanced.
- Expliquer comment le déploiement centralisé via AWS Firewall Manager peut améliorer la sécurité.

Travaux pratiques
Utilisation d'AWS WAF pour atténuer le trafic malveillant.

7 Surveillance et collecte des logs sur AWS

- Identifier l'importance de générer et de collecter des logs.
- Utiliser les logs de flux Amazon Virtual Private Cloud (Amazon VPC) pour surveiller les événements de sécurité.
- Expliquer comment surveiller les écarts par rapport à la ligne de base.
- Décrire les événements Amazon EventBridge.
- Décrire les métriques et les alarmes Amazon CloudWatch.
- Lister les options d'analyse des journaux et les techniques disponibles.
- Identifier les cas d'utilisation du miroir de trafic dans un cloud privé virtuel (VPC).

Travaux pratiques
Surveillance et réponse aux incidents de sécurité.

8 Répondre aux menaces

- Classer les types d'incidents dans la réponse aux incidents.
- Comprendre les flux de travail de la réponse aux incidents.
- Découvrir les sources d'informations pour la réponse aux incidents en utilisant les services AWS.
- Comprendre comment se préparer aux incidents.
- Détecter les menaces à l'aide des services AWS.
- Analyser et répondre aux résultats de sécurité.

Travaux pratiques
Réponse aux incidents

Options

Certification : 360 € HT

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).
Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE
2026 : 24 mars, 16 juin, 29 sep., 8 déc.

PARIS LA DÉFENSE
2026 : 24 mars, 16 juin, 29 sep., 8 déc.