Ingénierie de sécurité sur AWS

Durée: 3 Jours Réf de cours: GK3338

Résumé:

La sécurité est une préoccupation à la fois pour les clients du cloud et pour ceux qui envisagent de l'adopter. L'augmentation des cyberattaques et des fuites de données reste une priorité pour la plupart des employés de l'industrie.
Le cours d'ingénierie de la sécurité sur AWS répond à ces préoccupations en vous aidant à mieux comprendre comment interagir et créer avec Amazon Web Services (AWS) de manière sécurisée.
Dans ce cours, vous apprendrez à gérer les identités et les rôles, à gérer et à provisionner les comptes, et à surveiller l'activité des API pour détecter les anomalies. Vous apprendrez également comment protéger les données stockées sur AWS. Le cours explore comment vous pouvez générer, collecter et surveiller les journaux pour vous aider à identifier les incidents de sécurité. Enfin, vous examinerez la détection et l'enquête sur les incidents de sécurité avec les services AWS.

Niveau du cours : Intermédiaire

Financement :
Formation éligible au Compte Personnel de Formation (CPF), permettant de préparer la Certification associée inscrite au répertoire de France Compétences.
La Certification professionnelle inscrite au Répertoire Spécifique de France Compétences RS5833 "Garantir la sécurité du cloud AWS" valable jusqu'au 26/01/2025.
Nous vous invitons à consulter les prérequis, les objectifs, le contexte de la certification ainsi que les détails de la certification sur :https://www.francecompetences.fr/recherche/rs/5833

Cette formation est également finançable au titre du dispositif action collective Cloud de l'Opco Atlas
Mise à jour : 20.01.2025

Public visé:

Ce cours s'adresse aux : Ingénieurs en sécurité, Architectes de sécurité, Architectes cloud, Opérateurs cloud.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Comprendre la sécurité du cloud AWS basée sur la triade de la CIA.
- Créer et analyser des authentifications et des autorisations avec IAM.
- Gérer et provisionner 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, Surveiller, générer et collecter des journaux.
- Identifier les services AWS qui traitent les attaques provenant de sources externes, les indicateurs d'incidents de sécurité, comment enquêter sur les menaces et les atténuer à l'aide des services AWS

Pré-requis:

Pour assister à cette formation, il est recommandé pour les candidats de:

- Posséder des connaissance des pratiques de sécurité dans le domaine de l'informatique en général
- Avoir suivi le cours GK4502 «Architecture sur AWS»
- D'avoir de l'expérience en gouvernance, évaluation du risque, en contrôle, et de conformité aux normes

Avez-vous les compétences requises pour cette formation ?
Testez vos connaissances !

Test et certification

Cette formation permet de préparer l'examen de certification **Specialty AWS Certified Security** (certification éditeur).

Cette formation mène également à la Certification professionnelle inscrite au Répertoire Spécifique de France Compétences RS5833 "Garantir la sécurité du cloud AWS". Plus de détails sur : https://www.francecompetences.fr/recherche/rs/5833/

Contenu:

Jour 1

Module 1 : Présentation et examen de la sécurité

- Expliquer la sécurité dans le cloud AWS.
- Expliquer le modèle de responsabilité partagée AWS.
- Résumez l'IAM, la protection des données et la détection et la réponse aux menaces.
- Indiquer les différentes façons d'interagir avec AWS à l'aide de la console, de l'interface de ligne de commande et des kits SDK.
- Décrire comment utiliser l'authentification multifacteur pour une protection supplémentaire.
- Indiquer comment protéger le compte d'utilisateur racine et les clés d'accès.

Module 2 : Sécurisation des points d'entrée sur AWS

- Décrire comment utiliser l'authentification multifacteur (MFA) pour une protection supplémentaire.
- Décrire comment protéger le compte d'utilisateur racine et les clés d'accès.
- Décrire les stratégies IAM, les rôles, les composants de stratégie et les limites d'autorisation.
- Expliquer comment les demandes d'API peuvent être enregistrées et affichées à l'aide d'AWS CloudTrail, et comment afficher et analyser l'historique d'accès.
- Atelier pratique : Utilisation des stratégies basées sur l'identité et les ressources.

Module 3 : Gestion et mise en service des comptes sur AWS

- Expliquer comment gérer plusieurs comptes AWS à l'aide d'AWS Organizations et d'AWS Control Tower.
- Expliquer comment mettre en œuvre des environnements multicomptes avec AWS Control Tower.
- Démontrer la capacité à utiliser des fournisseurs d'identité et des courtiers pour obtenir l'accès 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 du domaine à l'aide du service d'annuaire et du centre d'identité IAM.
- Atelier pratique : Gestion de l'accès des utilisateurs au domaine avec AWS Directory Service

Jour 2

Module 4 : Gestion des secrets sur AWS

- Décrire et répertorier les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager.
- Démonstration de la création d'une clé AWS KMS multi-régions.
- Démonstration du chiffrement d'un secret Secrets Manager à l'aide d'une clé AWS KMS.
- Démonstration de l'utilisation d'une clé secrète chiffrée pour se connecter à une base de données Amazon Relational Database Service (Amazon RDS) dans plusieurs régions AWS
- Atelier pratique : Utilisation d'AWS KMS pour chiffrer les secrets dans Secrets Manager

Module 5 : Sécurité des données

- Surveiller les données à la recherche d'informations sensibles avec Amazon Macie.
- Décrire comment protéger les données au repos par le chiffrement et les contrôles d'accès.
- Identifier les services AWS utilisés pour répliquer les données à des fins de protection.
- Déterminer comment protéger les données une fois qu'elles ont été archivées.
- Atelier pratique : Sécurité des données dans Amazon S3

Module 6 : Protection des bords de l'infrastructure

- Décrire les fonctionnalités AWS utilisées pour créer 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 d'AWS Firewall Manager peut améliorer la sécurité.
- Atelier pratique : Utilisation d'AWS WAF pour atténuer le trafic malveillant

Jour 3

Module 7 : Surveillance et collecte des journaux sur AWS

- Identifier la valeur de la génération et de la collecte des journaux.
- Utiliser les journaux de flux Amazon Virtual Private Cloud (Amazon VPC) pour surveiller les événements de sécurité.
- Expliquer comment surveiller les écarts de référence.
- Décrire les événements Amazon EventBridge.
- Décrire les métriques et les alarmes Amazon CloudWatch.
- Énumérer les options d'analyse des journaux et les techniques disponibles.
- Identifier les cas d'utilisation de la mise en miroir du trafic VPC (Virtual Private Cloud).
- Atelier pratique : Surveillance et réponse aux incidents de sécurité

Module 8 : Réagir aux menaces

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

Atelier pratique : Réponse aux incidents

Méthodes pédagogiques :

Méthodes pédagogiques : Un support de cours est remis à chaque participant au format électronique Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation. Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.

Autres moyens pédagogiques et de suivi : Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique. Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur. Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés. Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations. A l'issue de cette session, chaque stagiaire bénéficiaire sera contacté par un prestataire choisi par l'Opco Atlas afin d'évaluer « à chaud » la qualité de la formation suivie.
Délais d'inscription : Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant. Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel. Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.
Financement : Formation éligible au Compte Personnel de Formation (CPF), permettant de préparer la Certification associée inscrite au répertoire de France Compétences. La Certification professionnelle inscrite au Répertoire Spécifique de France Compétences RS5849 "Mettre en œuvre DevOps pour le cloud AWS" valable jusqu'au 26/01/2025

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form"""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement