Security Engineering on AWS – Formation intensive («AWSS04»)

Grâce à cette formation de niveau intermédiaire, apprenez à utiliser les services de sécurité AWS pour assurer la sécurité des données dans le Cloud AWS. Ce cours marque une étape essentielle vers la certification « AWS Certified Security – Specialty ».

Durée: 3 jours
Prix : 2'500.– excl. 8.1% TVA
Documents : Support électronique officiel AWS
Code officiel: AWSS04

Contenu

Ce cours met en lumière les fonctionnalités de sécurité intégrées aux principaux services AWS, notamment les services de calcul, de stockage, de mise en réseau et de base de données. Ce cours aborde également les objectifs courants en matière de contrôle de la sécurité et les normes réglementaires de mise en conformité, et examine des cas d'utilisation de charges de travail réglementées sur AWS, dans différents secteurs d'activité aux quatre coins du monde. Vous découvrirez également comment tirer parti des services et outils AWS pour automatiser et contrôler vos activités en continu, et amener ainsi vos opérations de sécurité au niveau supérieur.

Jour 1
Module 1 : Aperçu et revue de la sécurité

- Expliquer la sécurité dans le cloud AWS
- Expliquer le modèle de responsabilité partagée AWS
- Résumer IAM, la protection des données, la détection des menaces et la réponse vis-à-vis des menaces
- Expliquer les différentes manières d'interagir avec AWS avec la console, CLI et les SDK
- Décrire comment utiliser la MFA pour augmenter la protection
- Expliquer comment protéger le compte utilisateur root et les clés d'accès

Module 2 : Sécuriser les points d'accès sur AWS

- Décrire comment utiliser l'authentification multifacteur (MFA) pour augmenter la protection
- Décrire comment protéger le compte utilisateur root et les clés d'accès
- Décrire les règles, rôles et limites de permission IAM
- Expliquer comment les requêtes API peuvent être journalisées et consultées avec AWS CloudTrail et comment consulter et analyser l'historique d'accès.
- Exercice pratique : Utiliser l'identité et les règles basées sur les ressources.

Module 3 : La gestion des comptes et l'approvisionnement sur AWS

- Expliquer comment gérer plusieurs comptes AWS avec AWS Organizations et AWS Control Tower
- Expliquer comment mettre en œuvre des environnements multicomptes avec AWS Control Tower
- Démontrer sa capacité à utiliser les fournisseurs d'identité pour avoir accès aux services AWS
- Expliquer l'utilisation d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) et AWS Directory Service
- Démontrer sa capacité à gérer l'accès des utilisateurs du domaine avec Directory Services et IAM Identity Center
- Exercice pratique : Gérer l'accès des utilisateurs du domaine avec AWS Directory Service

Jour 2

Module 4 : Gérer les secrets sur AWS

- Décrire et lister les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager
- Comment créer une clé AWS KMS multirégion
- Comment chiffrer un secret Secrets Manager avec une clé AWS KMS
- Comment utiliser un secret chiffré pour se connecter à une base de données Amazon Relaional Database Service (Amazon RDS) dans plusieurs régions AWS
- Exercice pratique : Exercice 3 : Utiliser AWS KMS pour chiffrer des secrets dans Secrets Manager

Module 5 : La sécurité des données

- Surveiller les données pour repérer des données sensibles avec Amazon Macie
- Comment protéger des données au repos grâce à chiffrement et au contrôle des accès
- Identifier les services AWS utilisés pour reproduire des données pour les protéger
- Comment protéger des données après archivage
- Exercice pratique : Exercice 4 : La sécurité des données dans Amazon S3

Module 6 : Protection de l'infrastructure de périphérie (Edge)

- Décrire les fonctionnalités AWS utilisées pour construire des infrastructures sécurisées
- Décrire les services AWS utilisés pour créer de la résilience face aux attaques
- Identifier les services AWS utilisés pour protéger les charges de travails de menaces externes
- Comparer les fonctionnalités d'AWS Shield et AWS Shield Advanced
- Expliquer comment centraliser le déploiement d'AWS Firewall Manager peut améliorer la sécurité
- Exercice pratique : Exercice 5 : Utiliser AWS WAF pour diminuer le trafic malveillant

Jour 3

Module 7 : Surveiller et collecter les fichiers journaux (logs) sur AWS

- Identifier la valeur de la création et de la collecte de fichiers journaux
- Utiliser Amazon Virtual Private Cloud (Amazon VPC) Flow Logs pour surveiller les événements liés à la sécurité
- Expliquer comment surveiller pour repérer des écarts par rapport au niveau de référence
- Décrire les événements Amazon EventBridge
- Décrire les métriques et alarmes Amazon CloudWatch
- Liste des options et des techniques disponibles pour l'analyse des fichiers journaux
- Identifier des cas d'utilisation de la mise en miroir du trafic Amazon VPC
- Exercice pratique : Exercice 6 : Surveiller et répondre à des incidents de sécurité

Module 8 : Répondre aux menaces

- Classer les types d'incidents dans la réponse aux incidents
- Comprendre les flux de travail de la réponse à un incident
- Découvrir les sources d'information pour la réponse aux incidents avec les services AWS
- Comprendre comment se préparer à un incident
- Détecter des menaces avec les services AWS
- Analyser et répondre aux constatations relatives à la sécurité
- Exercice pratique : Exercice 7 : Réponse aux incidents

Objectifs

- Comprendre la sécurité du cloud AWS en se basant sur la confidentialité, l'intégrité et la disponibilité
- Créer et analyser l'authentification et les autorisations avec IAM
- Gérer et fournir des comptes sur AWS avec les services AWS appropriés
- Identifier comment gérer les secrets en utilisant les services AWS
- Surveiller les informations sensibles et protéger les données grâce au chiffrement et au contrôle des accès
- Identifier les services AWS qui répondent aux attaques de sources externes
- Surveiller, générer et collecter des fichiers journaux
- Identifier les indicateurs d'incidents de sécurité
- Identifier comment évaluer les menaces et les atténuer grâce aux services AWS

Méthodologie & Didactique

Ce cours est une formation intensive sous forme de bloc de sessions journalières, si vous préférez un format plus flexible, sous forme de plusieurs sessions virtuelles de 3 heures sur plusieurs jours, cliquez ici.

Ce cours comprend des présentations, des exercices pratiques, des démos et des exercices en groupe.

Public cible

Ce cours s'adresse aux Ingénieurs en sécurité, Architectes en sécurité, Analystes en sécurité, Auditeurs en sécurité et personnes chargées de la gouvernance, de l'audit et du test de l'infrastructure informatique d'une organisation, et garantissant la conformité de l'infrastructure à l'égard des directives en matière de sécurité, de risques et de mise en conformité.

Pourquoi suivre ce cours en particulier ? Quels sont les avantages de ce cours ? **Nos formatrices et formateurs répondent à ces questions**. Nous avons demandé à notre équipe de formatrices et formateurs d'écrire un petit texte qui explique POURQUOI la formation est particulièrement importante pour le rôle professionnel et ce qui peut être attendu du cours. Vous trouverez ces informations dans la description du cours sous la rubrique « informations complémentaires ».

Prérequis

Les participantes et participants doivent avoir au préalable :

- Suivi les cours suivants :
  - AWS Security Essentials ou
  - AWS Security Fundamentals et
  - Architecting on AWS
- Des connaissances pratiques des procédés de sécurité informatique et des concepts d'infrastructure
- Des connaissances générales du cloud AWS

- AWS Security Essentials – Formation intensive («AWSE04»)
- Architecting on AWS – Formation intensive («AWSA01»)

Certification

Cette formation marque une étape essentielle vers la certification « AWS Certified Security – Specialty » pour laquelle il faut passer l'examen SCS-C01.

Nous vous conseillons également de suivre les formations suivantes afin de maîtriser toute la matière de l'examen :

- AWS Security Essentials
- AWS Security Best Practices
- AWS Security Governance at Scale

L'examen ne fait pas partie de la formation. Nous conseillons de vous inscrire à l'examen lorsque vous aurez au moins 5 ans d'expérience dans le domaine de la conception de solutions de sécurité informatique et au moins deux d'expérience avec la sécurisation des technologies AWS. L'examen, dont l'inscription se fait directement auprès d'AWS, dure 170 minutes et coûte USD 300.

Informations complémentaires

Paroles de formatrices et formateurs

Participer au cours « Security Engineering on AWS » est intéressant pour les personnes intéressées à améliorer leurs compétences et connaissances de la sécurité sur AWS. En voici les avantages principaux :

1. Expertise de la sécurité AWS : Ce cours explore en détail les services, outils et bonnes pratiques de sécurité sur AWS. Il permet d'acquérir les connaissances nécessaires à la conception, à la mise en œuvre et à la gestion d'applications et d'infrastructures sécurisées sur AWS.
2. Protection des données et des biens : AWS propose une large gamme de services et fonctionnalités de sécurité et ce cours vous aide à comprendre comment les exploiter de manière efficace. Vous découvrirez le cryptage, le contrôle des accès, la gestion des identités et des accès (IAM), la sécurité du réseau et les systèmes de protection des données qui permettent de protéger les données et les biens sensibles sur AWS.
3. Conformité et gouvernance : Comprendre les exigences en matière de conformité et mettre en œuvre des contrôles appropriés est particulièrement important pour de nombreuses entreprises. Cette formation vous aide à aligner vos déploiements d'AWS avec les standards et bonnes pratiques de l'industrie.
4. Réponse aux incidents et contrôle : Des incidents de sécurité peuvent survenir malgré les mesures préventives. Ce cours explore les stratégies de réponse aux incidents, la détection des menaces et les techniques de contrôle avec des services AWS tels que AWS CloudTrail, AWS Config et Amazon GuardDuty. Vous aurez un aperçu complet de la manière d'identifier et répondre rapidement à des événements portant atteinte à la sécurité.
5. Les besoins de l'industrie et les opportunités professionnelles : Avec l'adoption croissante d'AWS dans les entreprises du monde entier, la demande en professionnel qualifié capable d'assurer la sécurité de déploiements d'AWS ne fait qu'augmenter. En suivant cette formation, vous vous positionnez en tant qu'ingénieur sécurité qualifié avec une large expérience d'AWS, ce qui vous permet d'élargir votre spectre de possibilités professionnelles dans ce domaine.
6. Expérience pratique : Ce cours comprend de nombreux exercices pratiques, labs et scénarios réels, ce qui vous permet de mettre en pratique les concepts appris. Cette expérience pratique vous octroie la confiance et l'expertise pour gérer les défis sécuritaires de manière efficace dans un environnement AWS.
7. Préparation à une certification AWS : Les connaissances acquises pendant le cours représentent le socle de connaissances de base qui mènent à la certification AWS Certified Security – Specialty. Cette certification professionnelle valide votre expertise en sécurisation d'environnements AWS et ajoute une certaine crédibilité à votre profil.

Pour résumer, participer au cours « Security Engineering on AWS » vous permet d'acquérir les compétences, les connaissances et l'expérience pratique nécessaire à la sécurisation efficace de déploiements d'AWS. Il ne développe pas seulement vos compétences professionnelles, mais vous permet également de contribuer à une implémentation sécurisée et réussie des solutions AWS.

Matériel

- **Support de cours :** Environ une semaine avant le début de votre formation, vous recevrez vos données d'accès (code voucher) aux supports de cours électroniques par e-mail directement de l'adresse noreply@gilmore.ca. Tous les supports de cours sont hébergés sur la plateforme evantage.gilmoreglobal.com. Veuillez suivre les instructions contenues dans l'e-mail et créer un compte avec votre adresse e-mail professionnelle (si vous n'avez pas encore de compte) pour accéder aux supports de cours.
- **Labs :** Tous les exercices des formations techniques sont hébergés sur la plateforme d'exercice officielle d'AWS digicomp.qwiklabs.com. Au début de leur formation, les participantes et participants devront créer leur propre compte sur digicomp.qwiklabs.com avec leur adresse e-mail professionnelle pour avoir accès aux labs officiels d'AWS et pouvoir effectuer les exercices pratiques.
- **Plateforme de formation :** Si vous participez à une formation virtuelle, vous recevrez l'accès à la plateforme de formation de Digicomp un jour avant le début de votre formation.
- Pour accéder aux supports de cours et exercices pendant le cours, pensez à les télécharger et à apporter votre propre tablette ou ordinateur portable.

Formations complémentaires

- Security Engineering on AWS – JAM Day («AWSSJ4»)
- AWS Well-Architected Best Practices – Formation intensive («AWSE08»)

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-it-providers/amazon-web-services-aws/aws-data-engineer/cours-security-engineering-on-aws-formation-intensive-awss04