Formation Security Engineering on AWS

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La sécurité est une préoccupation à la fois pour les clients du cloud et pour ceux qui envisagent d'adopter le cloud. Une augmentation des cyberattaques et des fuites de données reste une préoccupation majeure pour la plupart des employés de l'industrie. Le cours Security Engineering on 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 de l'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 des journaux pour vous aider à identifier les incidents de sécurité. Enfin, vous passerez en revue la détection et l'investigation des incidents de sécurité avec les services AWS.

Référence	AWSSECENG
Durée	3 jours (21h)
Tarif	2 100 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 12 au 14 juin 2024
du 21 au 23 août 2024
du 23 au 25 octobre 2024
du 11 au 13 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| Énoncer une compréhension de la sécurité du cloud AWS basée sur la triade CIA.
| Créer et analyser l'authentification et les autorisations avec IAM.
| Gérer des comptes sur AWS avec les services AWS appropriés.
| Identifier comment gérer les secrets à l'aide des services AWS.
| Protéger les données via le cryptage et les contrôles d'accès.
| Identifier les services AWS qui traitent les attaques provenant de sources externes.
| Surveiller, générer et collecter des journaux.
| Identifier les indicateurs d'incidents de sécurité.
| Enquêter sur les menaces et les atténuer à l'aide des services AWS.

Prérequis

| Avoir suivi les cours suivants
| AWS Security Essentials
| Architecting on AWS

| Posséder une connaissance opérationnelle des pratiques de sécurité informatique et des concepts d'infrastructure.

Public

| Ingénieurs en sécurité
| Architectes de sécurité
| Architectes Cloud

Programme de la formation

Présentation et examen de la sécurité
| Expliquer la sécurité dans le cloud AWS.
| Expliquer le modèle de responsabilité partagée AWS.
| Résumer l'IAM, la protection des données et la détection et la réponse aux menaces.
| Indiquer les différentes manières d'interagir avec AWS à l'aide de la console, de l'interface de ligne de commande et des SDK.

| Décrire comment utiliser MFA pour une protection supplémentaire.
| Indiquer comment protéger le compte utilisateur root et les clés d'accès.

Sécurisation des points d'entrée sur AWS
| Décrire comment utiliser l'authentification multifacteur (MFA) pour une protection supplémentaire.
| Décrire comment protéger le compte utilisateur root 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 des accès.
| Mise en pratique : Utilisation de stratégies basées sur l'identité et les ressources.

Gestion de compte et provisionnement sur AWS
| Expliquer comment gérer plusieurs comptes AWS à l'aide d'AWS Organizations et d'AWS Control Tower.
| Expliquer comment mettre en oeuvre des environnements multi-comptes avec AWS Control Tower.
| Démontrer la capacité à utiliser des fournisseurs d'identité et des courtiers pour acquérir 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 de domaine avec Directory Service et IAM Identity Center.
| Mise en pratique : Gestion de l'accès des utilisateurs au domaine avec AWS Directory Service

Gestion des secrets sur AWS
| Décrire et répertorier les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et Gestionnaire de secrets AWS.
| Montrer comment créer une clé AWS KMS multirégionale.
| Montrer comment chiffrer un secret Secrets Manager avec une clé AWS KMS.
| Démontrer comment utiliser un secret chiffré pour se connecter à une base de données Amazon Relational Database Service (Amazon RDS) dans plusieurs régions AWS
| Mise en pratique : Atelier 3 : Utilisation d'AWS KMS pour chiffrer des secrets dans Secrets Manager

Sécurité des données
| Surveiller les données pour les informations sensibles avec Amazon Macie.
| Décrire 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 après leur archivage.
| Mise en pratique : Atelier 4 : Sécurité des données dans Amazon S3

Protection de la périphérie 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.
| Mise en pratique : Atelier 5 : Utilisation d'AWS WAF pour atténuer le trafic malveillant

Surveillance et collecte de journaux sur AWS
| Identifier la valeur de la génération et de la collecte des logs.
| 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.
| Liste des options d'analyse des journaux et des techniques disponibles.
| Identifier les cas d'utilisation pour l'utilisation de la mise en miroir du trafic du cloud privé virtuel (VPC).
| Mise en pratique : Laboratoire 6 : Surveillance et réponse aux incidents de sécurité

Répondre 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 et répondre aux constatations de sécurité.
| Mise en pratique : Réponse aux incidents

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.