DAWAN

Plan de la formation

www.dawan.fr

Formation Security Engineering on AWS

Durée :	3 jours (21 heures)
Tarif inter-entreprise :	2 775,00 CHF HT (standard) 2 220,00 CHF HT (remisé)
Public :	Ingénieurs sécurité, architectes sécurité et professionnels de la sécurité de l'information
Pré-requis :	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.
Objectifs :	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 - Être préparé à l’examen officiel AWS Certified Security – Specialty
Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CLO102958-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre la sécurité du cloud AWS selon le modèle CIA

Replacer la sécurité AWS dans les principes de confidentialité, intégrité et disponibilité
Comprendre les spécificités de la sécurité dans un environnement cloud
Appliquer le modèle de responsabilité partagée à différents cas d’usage
Relier les objectifs de sécurité aux services et mécanismes proposés par AWS
Identifier les grands domaines de sécurisation d’un environnement cloud
Mettre en relation architecture, exploitation et gouvernance de la sécurité

Atelier fil rouge
Analyser une architecture AWS simple au regard des exigences de confidentialité, d’intégrité et de disponibilité

Créer et analyser des authentifications et des autorisations avec IAM

Comprendre les concepts fondamentaux d’IAM
Structurer les identités, rôles, groupes, politiques et permissions
Appliquer les principes de moindre privilège et de séparation des rôles
Mettre en place une lecture de la fédération et des accès multi-comptes

Identifier les erreurs fréquentes dans la gestion des permissions
Vérifier la cohérence d'une stratégie d'authentification et d'autorisation

Atelier fil rouge
Construire une stratégie IAM simple et analyser les écarts de sécurité dans des politiques d'accès

Gérer et approvisionner des comptes sur AWS avec les services AWS appropriés

Comprendre l'organisation multi-comptes dans AWS
Identifier les services et méthodes de gouvernance adaptés à l'approvisionnement de comptes
Structurer une organisation cohérente pour limiter les risques et améliorer la maîtrise
Relier la gestion des comptes à la supervision, à la conformité et au pilotage des accès
Intégrer les principes de segmentation et d'isolement des environnements
Prendre en compte les besoins d'exploitation et d'audit

Atelier fil rouge
Définir une organisation multi-comptes pour une entreprise souhaitant cloisonner ses environnements et renforcer sa gouvernance

Gérer les secrets et protéger les données via le cryptage et les contrôles d'accès

Identifier les besoins de gestion des secrets dans une architecture AWS
Comprendre la logique de protection des données au repos et en transit
Mettre en relation les mécanismes de chiffrement avec les exigences réglementaires et opérationnelles
Définir les bons niveaux de contrôle d'accès selon les types de données
Identifier les points de vigilance liés aux clés, certificats et secrets d'application
Articuler protection des données, sécurité des accès et exploitation

Atelier fil rouge
Qualifier les mécanismes de protection adaptés à plusieurs catégories de données dans un environnement AWS

Identifier les services AWS qui répondent aux attaques provenant de sources externes

Comprendre les principales menaces externes pesant sur des environnements exposés
Identifier les familles de services AWS contribuant à la protection des réseaux,

applications et interfaces publiques
Mettre en relation sécurité périmétrique, défense applicative et capacité de réaction
Évaluer les choix de protection selon le niveau d'exposition et de criticité
Intégrer la défense contre les attaques dans une logique globale d'architecture sécurisée
Repérer les limites d'une approche purement technique

Atelier fil rouge
Proposer des mesures de protection adaptées à une application AWS exposée à Internet

Surveiller, générer et collecter les logs

Comprendre le rôle de la journalisation dans la sécurité cloud
Identifier les sources de logs utiles à la détection et à l'investigation
Structurer une démarche de collecte, centralisation et exploitation des événements
Relier supervision, détection et amélioration continue
Définir les critères de qualité d'une stratégie de journalisation
Prendre en compte les besoins d'audit et de conformité

Atelier fil rouge
Élaborer une stratégie simple de journalisation et de suivi de sécurité pour un environnement AWS

Identifier les indicateurs d'incidents de sécurité

Reconnaître les signaux faibles et les événements significatifs
Qualifier les comportements anormaux sur les accès, les ressources ou les données
Relier les indicateurs techniques à une logique de détection opérationnelle
Prioriser les événements à analyser selon le niveau de risque
Distinguer alerte technique, incident avéré et faux positif
Mettre en place une lecture structurée des signaux de sécurité

Atelier fil rouge
Analyser un ensemble d'événements de sécurité et identifier les indicateurs justifiant une investigation

Enquêter sur les menaces et les atténuer à l'aide des services AWS

Organiser une première démarche d'investigation sur un incident de sécurité
Qualifier les impacts potentiels et les mesures immédiates de réduction du risque
Identifier les services AWS utiles à l'analyse, à la réponse et à la remédiation

Structurer un raisonnement d’atténuation cohérent avec le contexte d’exploitation
Contribuer à une logique de retour d’expérience et d’amélioration continue
Relier réponse à incident, architecture et gouvernance de sécurité

Atelier fil rouge
Traiter un scénario d’incident de sécurité AWS depuis l’identification des signaux jusqu’aux premières mesures d’atténuation

Se préparer à l’examen officiel AWS Certified Security – Specialty

Comprendre la structure et le niveau d’exigence de l’examen
Identifier les domaines couverts et les raisonnements attendus
S’entraîner à traiter des questions scénarisées orientées sécurité AWS
Repérer les pièges d’interprétation fréquents
Adopter une méthode de lecture et de décision adaptée au niveau Specialty
Consolider les axes de révision prioritaires

Atelier fil rouge
Réaliser un entraînement guidé sur des questions de niveau AWS Certified Security – Specialty et corriger les réponses de manière argumentée