Security Engineering on AWS – Intensive Training («AWSS04»)

Dieser Kurs bereitet Sie darauf vor, ein AWS Certified Security (Specialty Level) zu werden. Sie lernen die von AWS empfohlenen Best Practices für Sicherheit kennen, um die Sicherheit Ihrer Daten und Systeme in der Cloud zu verbessern.

Dauer: 3 Tage
Preis: 2'500.– zzgl. 8.1% MWST
Kursdokumente: Digitale Original-AWS-Kursunterlagen
Herstellercode: AWSS04

Inhalt

Tag 1
Modul 1: Sicherheit auf AWS

- Sicherheit in der AWS Cloud
- AWS-Modell der geteilten Verantwortung
- Überblick über die Reaktion auf Vorfälle
- DevOps mit Sicherheitstechnik

Modul 2: Identifizierung von Einstiegspunkten in AWS

- Identifizieren der verschiedenen Zugangsmöglichkeiten zur AWS-Plattform
- Verstehen von IAM-Richtlinien
- IAM-Berechtigungsgrenze
- IAM-Zugriffs-Analysator
- Multi-Faktor-Authentifizierung
- AWS CloudTrail
- Übung 01: Kontoübergreifender Zugriff

Modul 3: Sicherheitserwägungen: Webanwendungs-Umgebungen

- Bedrohungen in einer dreistufigen Architektur
- Häufige Bedrohungen: Benutzerzugriff
- Gängige Bedrohungen: Datenzugriff
- AWS Trusted Advisor

Modul 4: Anwendungssicherheit

- Amazon Machine Images
- Amazon Inspektor
- AWS Systems Manager
- Übung 02: Verwendung von AWS Systems Manager und Amazon Inspector

Modul 5: Datensicherheit

- Strategien zum Schutz von Daten
- Verschlüsselung auf AWS
- Schutz von Daten im Ruhezustand mit Amazon S3, Amazon RDS, Amazon DynamoDB
- Schutz von archivierten Daten mit Amazon S3 Glacier
- Amazon S3 Access Analyzer
- Amazon-S3-Zugangspunkte

Tag 2

Modul 6: Absicherung der Netzwerkkommunikation

- Amazon-VPC-Sicherheitsüberlegungen
- Amazon-VPC-Verkehrsspiegelung
- Reagieren auf gefährdete Instanzen
- Elastischer Lastausgleich
- AWS-Zertifikat-Manager

Modul 7: Überwachung und Erfassung von Protokollen auf AWS

- Amazon CloudWatch und CloudWatch-Protokolle
- AWS-Konfiguration
- Amazon Macie
- Amazon VPC-Flow-Protokolle
- Amazon S3 Server-Zugriffsprotokolle
- ELB-Zugriffsprotokolle
- Übung 03: Überwachen und Reagieren mit AWS Config

Modul 8: Verarbeitung von Protokollen auf AWS

- Amazon Kinesis
- Amazon Athena
- Übung 04: Webserver-Protokollanalyse

Modul 9: Sicherheits-Betrachtungen: Hybride Umgebungen

- AWS Site-to-Site- und Client-VPN-Verbindungen
- AWS Direktverbindung
- AWS Transit-Gateway

Modul 10: Out-of-Region-Schutz

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS-Schutzschild
- AWS-Firewall-Manager
- DDoS-Abwehr auf AWS

Tag 3

Modul 11: Sicherheitsüberlegungen: Serverlose Umgebungen

- Amazon Cognito
- Amazon API-Gateway
- AWS Lambda

Modul 12: Erkennung und Untersuchung von Bedrohungen

- Amazon GuardDuty
- AWS Sicherheits-Hub
- Amazon Detektiv

Modul 13: Verwaltung von Geheimnissen in AWS

- AWS KMS
- AWS CloudHSM
- AWS-Geheimnis-Manager
- Übung 05: Verwendung von AWS KMS

- AWS CloudFormation
- AWS Service-Katalog
- Übung 06: Sicherheitsautomatisierung auf AWS mit AWS Service Catalog

Modul 15: Kontoverwaltung und -bereitstellung in AWS

- AWS-Organisationen
- AWS-Kontrollturm
- AWS SSO
- AWS-Verzeichnisdienst
- Übung 07: Föderierter Zugriff mit ADFS

Key Learnings

- Identifizieren der Sicherheitsvorteile und Verantwortlichkeiten bei der Nutzung der AWS Cloud
- Aufbau sicherer Anwendungsinfrastrukturen
- Schutz von Anwendungen und Daten vor allgemeinen Sicherheitsbedrohungen
- Durchführen und Automatisieren von Sicherheitsüberprüfungen
- Konfigurieren von Authentifizierung und Berechtigungen für Anwendungen und Ressourcen
- Überwachen von AWS-Ressourcen und Reagieren auf Vorfälle
- Erfassen und Verarbeiten von Protokollen
- Erstellen und Konfigurieren automatisierter und wiederholbarer Bereitstellungen mit Tools wie AMIs und AWS CloudFormation

Methodik & Didaktik

Diese hybriden Kurse bestehen aus 3 ganztägigen Kursen, die von einem Trainer geleitet werden, der die Teilnehmenden direkt betreut. Jeder Kurs besteht aus theoretischen Teilen mit Live-Demonstrationen und praktischen Lab-Übungen. Der Kurs kann entweder vor Ort an einem Digicomp-Standort oder virtuell über Zoom besucht werden. Bitte beachten Sie die Beschreibung der einzelnen Kurse für spezifische Details bezüglich der Voraussetzungen und der behandelten Themen.

Zielpublikum

Dieser Kurs richtet sich an folgende Job-Rollen:

- Cyber Security
- Data Analytics

Warum sollten Sie an diesem Kurs teilnehmen? Welchen Nutzen bringt Ihnen diese Schulung? **The Voice of the Instructor beantwortet diese Fragen**. Wir haben unser Trainerteam gebeten, einen kurzen Text darüber zu verfassen, WARUM dieser Kurs für die jeweilige Jobrolle relevant ist und was Sie von der Teilnahme an diesem Kurs erwarten können. Sie finden diesen Abschnitt in der Kursbeschreibung unter *«Zusatzinfo»*.

Anforderungen

Es wird empfohlen, dass die Teilnehmenden den folgenden Kurs besucht haben (oder über gleichwertige Kenntnisse verfügen):

- Architecting on AWS – Intensive Training («AWSA01»)
- AWS Security Essentials – Intensive Training («AWSE04»)

Zusatzinfo

Die Teilnahme am Kurs «Security Engineering on AWS» bietet mehrere überzeugende Gründe für Personen, die ihre Fähigkeiten und Kenntnisse im Bereich AWS-Sicherheit erweitern möchten. Hier sind einige der wichtigsten Vorteile:

1. Umfassendes Wissen über AWS-Sicherheit: In diesem Kurs werden die AWS Security Services, Tools und Best Practices ausführlich behandelt. Er vermittelt Ihnen das Wissen, das Sie benötigen, um sichere Anwendungen und Infrastrukturen auf AWS zu entwickeln, zu implementieren und zu verwalten.
2. Schutz von Daten und Assets: AWS bietet ein robustes Set an Sicherheitsservices und -funktionen, und dieser Kurs hilft Ihnen zu verstehen, wie Sie diese effektiv nutzen können. Sie erfahren mehr über Verschlüsselung, Zugriffskontrolle, Identitäts- und Zugriffsmanagement (IAM), Netzwerksicherheit und Datenschutzmechanismen, damit Sie sensible Daten und Assets auf AWS schützen können.
3. Compliance und Governance: Das Verständnis der Compliance-Anforderungen und die Implementierung geeigneter Kontrollen sind für viele Unternehmen von entscheidender Bedeutung. Dieser Kurs unterstützt Sie dabei, Ihre AWS-Bereitstellungen an Branchenstandards und Best Practices auszurichten.
4. Incident Response und Monitoring: Trotz präventiver Massnahmen kann es zu Sicherheitsvorfällen kommen. Dieser Kurs behandelt Strategien zur Reaktion auf Vorfälle, Bedrohungserkennung und Überwachungstechniken unter Verwendung von AWS-Diensten wie AWS CloudTrail, AWS Config und Amazon GuardDuty. Sie erhalten Einblicke in die Identifizierung und Reaktion auf Sicherheitsereignisse in kürzester Zeit.
5. Branchenbedarf und Karrieremöglichkeiten: Mit der zunehmenden Nutzung von AWS durch Unternehmen weltweit steigt auch der Bedarf an qualifizierten Fachkräften, die die Sicherheit von AWS-Bereitstellungen gewährleisten können. Mit dem Abschluss dieses Kurses positionieren Sie sich als qualifizierter Sicherheitsingenieur mit AWS-Kenntnissen und erweitern Ihre Karrierechancen in diesem Bereich.
6. Praktische Erfahrung: Der Kurs beinhaltet praktische Übungen und reale Szenarien, die es Ihnen ermöglichen, die erlernten Konzepte in der Praxis anzuwenden. Diese praktische Erfahrung gibt Ihnen das Selbstvertrauen und die Fähigkeit, Sicherheitsherausforderungen in einer AWS-Umgebung effektiv zu bewältigen.
7. Vorbereitung auf die AWS-Zertifizierung: Das in diesem Kurs erworbene Wissen dient als solide Grundlage für die «AWS Certified Security – Specialty»-Zertifizierung. Diese professionelle Zertifizierung bestätigt Ihre Kompetenz in der Absicherung von AWS-Umgebungen und verleiht Ihrem Profil Glaubwürdigkeit.

Insgesamt vermittelt Ihnen die Teilnahme am Kurs «Security Engineering on AWS» die notwendigen Fähigkeiten, Kenntnisse und praktischen Erfahrungen, um AWS-Bereitstellungen effektiv abzusichern. Der Kurs erweitert nicht nur Ihre fachlichen Kompetenzen, sondern befähigt Sie auch, zur sicheren und erfolgreichen Implementierung von AWS-Lösungen beizutragen.

Weiterführende Kurse

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

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-it-provider/amazon-web-services-aws/aws-cyber-security/kurs-security-engineering-on-aws-intensive-training-awss04