Security Engineering on AWS (AWS-SO)

Im Kurs "Sicherheitsvorgänge in AWS" wird erläutert, wie AWS-Sicherheitsservices effizient zur Bewahrung von Sicherheit und Compliance in der AWS-Cloud genutzt werden können. Der Schwerpunkt liegt auf den von AWS empfohlenen, bewährten Sicherheitsmethoden, die für höhere Sicherheit Ihrer Daten und Systeme in der Cloud sorgen. Der Kurs beleuchtet die Sicherheitsfunktionen wichtiger AWS-Services wie Datenverarbeitungs-, Speicher-, Netzwerk- und Datenbankservices. Er behandelt auch die üblichen Sicherheitskontrollziele und die Standards zur Einhaltung gesetzlicher Vorschriften und erläutert Anwendungsfälle für laufende regulierte Verarbeitungslasten auf AWS für verschiedene Branchen weltweit. Außerdem lernen Sie, wie man AWS-Services und -Tools zur Automatisierung und fortlaufenden Überwachung nutzt - und dadurch Sicherheitsvorgänge zuverlässiger macht denn je.

Das Seminar führen wir in Zusammenarbeit mit unserem zertifizierten Partner Fast Lane durch.

Listenpreis

2.685,00 € exkl. MwSt

3.195,15 € inkl. MwSt

Dauer

3 Tage

Gebühr für Prüfungen/Examen

320,00 € exkl. MwSt / 380,80 € inkl. MwSt

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin

Gabriela Bücherl
Geschäftsführung
Vertrieb

Kontakt/Fragen:
g.buecherl@cbt-training.de
Telefon: +49 (0)89-4576918-16

Inhalte

1. Tag

- **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 bei AWSdie verschiedenen Möglichkeiten des Zugriffs auf die AWS-Plattform zu identifizieren**
  - Verstehen von IAM-Richtlinien
  - IAM-Berechtigungsgrenze
  - IAM Access Analyzer
  - Multi-Faktor-Authentifizierung
  - AWS CloudTrail
  - Übung 01: Kontoübergreifender Zugriff
- **Modul 3: Sicherheitserwägungen:**
  - Webanwendungsumgebungen
  - Bedrohungen in einer dreistufigen Architektur
  - Häufige Bedrohungen: Benutzerzugang
  - Häufige Bedrohungen: Datenzugang
  - AWS Trusted Advisor
- **Modul 4: Anwendungssicherheit**
  - Amazonas Maschine Bilder

- Amazonas-Inspektor
- AWS-Systemmanager
- 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: Sicherung der Netzwerkkommunikation**
  - Sicherheitsüberlegungen zu Amazon VPC
  - 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
  - Amazone Macie
  - Amazon VPC-Ablaufprotokolle
  - Amazon S3 Server-Zugriffsprotokolle
  - ELB-Zugriffsprotokolle
  - Übung 03: Überwachen und Reagieren mit AWS Config
- **Modul 8: Verarbeitung von Protokollen auf AWS**
  - Amazonas Kinesis
  - Amazonas-Athena
  - Lab 04: Web Server Log Analysis
- **Modul 9: Sicherheitserwägungen: Hybride Umgebungen**
  - AWS Site-to-Site- und Client-VPN-Verbindungen
  - AWS-Direktverbindung
  - AWS-Transit-Gateway
- **Modul 10: Schutz außerhalb der Region (Out-of-Region)**
  - Amazon Route 53
  - AWS WAF
  - Amazon CloudFront
  - AWS-Schild
  - AWS Firewall Manager
  - DDoS-Abwehr auf AWS

Tag 3

- **Modul 11: Sicherheitsüberlegungen: Serverlose Umgebungen**
  - Amazonas Kognito
  - Amazon API-Gateway
  - AWS Lambda
- **Modul 12: Erkennen und Untersuchen von Bedrohungen**
  - Amazon GuardDuty
  - AWS-Sicherheits-Hub
  - Amazonas-Detektiv
- **Modul 13: Verwaltung von Geheimnissen auf AWS**

  - AWS KMS
  - AWS CloudHSM
  - AWS-Geheimnis-Manager
  - Übung 05: AWS KMS verwenden
- **Modul 14: Automatisierung und Sicherheit durch Design**
  - AWS CloudFormation
  - AWS-Servicekatalog
  - Übung 06: Sicherheitsautomatisierung auf AWS mit AWS Service Catalog
- **Modul 15: Kontoverwaltung und -bereitstellung auf AWS**
  - AWS-Organisationen
  - AWS-Kontrollturm
  - AWS SSO
  - AWS-Verzeichnisdienst
  - Übung 07: Föderierter Zugriff mit ADFS

Ziele

- Identifizierung der Sicherheitsvorteile und Verantwortlichkeiten bei der Nutzung der AWS-Cloud
- Aufbau sicherer Anwendungsinfrastrukturen
- Schutz von Anwendungen und Daten vor gängigen Sicherheitsbedrohungen
- Sicherheitsüberprüfungen durchführen und automatisieren
- Konfigurieren Sie die Authentifizierung und Berechtigungen für Anwendungen und Ressourcen
- AWS-Ressourcen überwachen und auf Vorfälle reagieren
- Erfassen und Verarbeiten von Protokollen
- Erstellen und Konfigurieren automatisierter und wiederholbarer Bereitstellungen mit Tools wie AMIs und AWS CloudFormation

---

Zielgruppe

- Sicherheitsingenieure
- Sicherheitsarchitekten
- Informationssicherheitsexperten

Voraussetzungen

- Absolvierung des Kurses "AWS Security Essentials" und "Architecting on AWS"
- Kenntnisse von IT-Sicherheitspraktiken
- Praktische Erfahrung mit IT-Infrastrukturkonzepten
- Vertrautheit mit Cloud Computing-Konzepten

Prüfung/Zertifizierung

AWS Certified Security - Specialty
