AW261 Security Engineering on AWS

Kurzbeschreibung:

AW410 Security Engineering on AWS ist ein dreitägiger Kurs, der den Teilnehmern die AWS-Sicherheitsdienste vorstellt und deren Nutzen in Bezug auf Sicherheit und Compliance erläutert. Dabei werden vor allem die von AWS empfohlenen Sicherheitsmethoden behandelt, mit denen eine erhöhte Sicherheit von Daten und Systemen in der Cloud erreicht werden kann: Sicherheitsfunktionen wichtiger Services aus dem Bereich Datenverarbeitung, Speicher, Netzwerk und Datenbanken, die von AWS angeboten werden, werden ebenso vorgestellt, wie der Umgang mit Sicherheitskontrollzielen und Standards zur Einhaltung gesetzlicher Vorschriften.

Anwendungsfälle aus verschiedenen Branchen geben einen Einblick in die kontinuierlich regulierten Verarbeitungslasten auf AWS. Die Vorstellung verschiedener AWS-Tools und -Services, die zur Automatisierung, Überwachung und Protokollierung sowie zur Reaktion auf Sicherheitsvorfälle genutzt werden können, rundet diesen Kurs ab.

Der Workshop setzt sich aus einer Präsentation und Übungen zusammen, um das Erlernte praktisch anzuwenden. Die Kursunterlagen (E-Book) sind in englischer Sprache, die Kurssprache ist deutsch.

Der Workshop „Security Engineering on AWS“ unterstützt Sie bei der Vorbereitung auf folgende Prüfung: **AWS Certified Security – Specialty**

Zielgruppe:

- Sicherheitsfachleute
- Sicherheitsarchitekten
- Sicherheitsanalysten
- Sicherheitsprüfer
- Für die Leitung, Überwachung und das Testen der IT-Infrastruktur einer Organisation sowie die Sicherstellung von deren Konformität mit Sicherheits-, Risiko- und Compliance-Richtlinien zuständige Personen

Voraussetzungen:

Um an dem Kurs **AW410 Security Engineering on AWS** bei qSkills teilnehmen zu können, sollten Sie das folgende AWS-Training besucht haben:

- „Security Fundamentals (digital)“
- "AWS Security Essentials"
- "Architecting on AWS"

Darüber hinaus sollten Sie folgende Voraussetzungen erfüllen:

- Erfahrung im Umgang mit Governance-, Risiko- und Compliance-Vorschriften sowie Kontrollzielen
- Praxiserfahrung im Umgang mit IT-Sicherheitsverfahren
- Praxiserfahrung im Umgang mit IT- Infrastrukturkonzepten
- Verständnis von Cloud Computing-Konzepten

Sonstiges:

Dauer: 3 Tage

Preis: 2685 Euro plus Mwst.

Ziele:

- Umfassendes Wissen zum Thema AWS-Cloud-Sicherheit in der AWS-Cloud auf Basis der CIA-Triade
- Erstellen und Analysieren von Authentifizierung sowie Berechtigungen mit IAM
- Verwalten und Bereitstellen von Konten auf AWS mit geeigneten AWS-Services
- Verwendung der Sicherheitsperspektive für die Verwaltung und Überwachung von AWS-Ressourcen
- Überwachung sensibler Informationen und Schutz von Daten durch Verschlüsselung und Zugriffskontrollen
- Kennenlernen von AWS-Services, die Angriffe von externen Quellen abwehren
- Überwachen, Erstellen und Sammeln von Protokollen
- Erkennen von Indikatoren für Sicherheitsvorfälle
- Bedrohungen untersuchen und mithilfe von AWS-Services entschärfen

Inhalte/Agenda:

- **Tag 1**
- **Modul 1: Security Overview and Review**
- **Modul 2: Securing Entry Points on AWS**
- ◊ Lab 1: Using Identity and Resource Based Policies.
- **Modul 3: Account Management and Provisioning on AWS**
- ◊ Lab 2: Managing Domain User Access with AWS Directory Service

- **Tag 2** ◊
- **Modul 4: Secrets management on AWS**
- ◊ Lab 3: Using AWS KMS to Encrypt Secrets in Secrets Manager
- **Modul 5: Data Security**
- ◊ Lab 4: Data Security in Amazon S3
- **Modul 6: Infrastructure Edge Protection**
- ◊ Lab 5: Using AWS WAF to Mitigate Malicious Traffic

- **Tag 3** ◊
- **Modul 7: Monitoring and Collecting Logs on AWS**
- ◊ Lab 6: Monitoring for and Responding to Security Incidents
- **Modul 8: Responding to Threats**
- ◊ Lab 7: Incident Response
- ◊