AW261-JAM Security Engineering on AWS with AWS Jam

Kurzbeschreibung:

Security- und Cloud-Professionals lernen Sicherheitsmethoden und -dienste auf AWS kennen und wenden ihr Wissen in einem AWS Jam Day mit praxisnahen Übungen an. Vermittelt werden Sicherheitsfunktionen für Datenverarbeitung, Speicher, Netzwerk und Datenbanken sowie der Umgang mit Sicherheitskontrollzielen und Standards. Behandelt wird zudem die Nutzung von AWS-Tools für Automatisierung, Monitoring, Protokollierung und Incident Response.

Zielgruppe:

Dieser Kurs **AW261-JAM Security Engineering on AWS with AWS Jam** richtet sich an:

- 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 **AW261-JAM Security Engineering on AWS with AWS Jam** bei qSkills teilnehmen zu können, sollten Sie das folgende AWS-Trainings besucht haben:

- Security Fundamentals (digital)
- AW120 AWS Security Essentials
- AW200 Architecting on AWS

Darüber hinaus sollten Sie folgende Voraussetzungen erfüllen:

- Praxiserfahrung im Umgang mit IT-Sicherheitsverfahren
- Praxiserfahrung im Umgang mit IT- Infrastrukturkonzepten
- Verständnis von Cloud Computing-Konzepten

Sonstiges:

Dauer: 4 Tage

Preis: 3175 Euro plus Mwst.

Ziele:

In diesem Kurs **AW261-JAM Security Engineering on AWS with AWS Jam** lernen Sie:

- Umfassendes Verständnis der 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**
  - ◊ Security Overview and Review
  - ◊ Securing Entry Points on AWS
  - ◊ Hands-On Lab: Using Identity and Resource Based Policies.
  - ◊ Account Management and Provisioning on AWS
  - ◊ Hands-On Lab: Managing Domain User Access with AWS Directory Service
  - ◊

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

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

- **Tag 4**
  - ◊ AWS Jam
    Teambasierte Herausforderungen in einer echten AWS-Umgebung lösen, in einem spielerischen, praxisnahen Lernprozess mit den Kollegen wetteifern und das erlernte Wissen auf verschiedene AWS-Services anwenden.
  - ◊