AW910 AWS Security Governance at Scale

Kurzbeschreibung:

Sicherheit ist ein grundlegendes Prinzip bei AWS. „Governance at Scale“ ist ein neues Konzept zur Automatisierung der Cloud-Governance, das Unternehmen dabei unterstützen kann, manuelle Prozesse in den Bereichen Account-Management, Budgetdurchsetzung sowie Sicherheit und Compliance abzulösen. Durch die Automatisierung gängiger Herausforderungen können Unternehmen skalieren, ohne Agilität, Geschwindigkeit oder Innovationsfähigkeit einzubüßen. Darüber hinaus können sie Entscheidungsträgern die notwendige Transparenz, Kontrolle und Governance bieten, um sensible Daten und Systeme zu schützen.

In diesem Kurs **AW910 AWS Security Governance at Scale** lernen Sie, wie Sie die Geschwindigkeit und Agilität von Entwicklern unterstützen und präventive sowie detektive Kontrollen integrieren. Am Ende dieses Kurses sind Sie in der Lage, Best Practices für Governance anzuwenden.

Der Kurs **AW910 AWS Security Governance at Scale** setzt sich aus einer Präsentation und Übungen zusammen, um das Erlernte gleich praktisch anzuwenden.

Zielgruppe:

Dieser Kurs **AW910 AWS Security Governance at Scale** richtet sich an:

- Solution Architects
- Security DevOps
- Security Engineers

Voraussetzungen:

Um an dem Kurs **AW910 AWS Security Governance at Scale** bei qSkills teilnehmen zu können, sollten Sie die folgenden AWS-Trainings besucht haben:

- Security Fundamentals
- AW120 AWS Security Essentials

Optional:

- AWS Cloud Management Assessment
- Introduction to AWS Control Tower
- Automated Landing Zone
- Introduction to AWS Service Catalog

Sonstiges:

Dauer: 1 Tage

Preis: 750 Euro plus Mwst.

Ziele:

In diesem Kurs **AW910 AWS Security Governance at Scale** lernen Sie:

- Eine Landing Zone mit AWS Control Tower einzurichten
- AWS Organizations zu konfigurieren, um eine Multi-Account-Umgebung zu erstellen
- Identitätsmanagement mit AWS Single Sign-On-Benutzern und -Gruppen zu implementieren
- Zugriffsföderation mit AWS SSO einzurichten
- Richtlinien mithilfe vordefinierter Guardrails durchzusetzen
- Zentrale Protokollierung mit AWS CloudTrail und AWS Config zu aktivieren
- Sicherheitsprüfungen über Kontengrenzen hinweg mit AWS Identity and Access Management (IAM) zu ermöglichen
- Workflows zur Bereitstellung von Accounts mit AWS Service Catalog und AWS Security Hub zu definieren

Inhalte/Agenda:

- ♦ **Kurseinführung**
  - ♦ ◊ Vorstellung der Trainerin oder des Trainers
    ◊ Lernziele
    ◊ Kursstruktur und Lernziele
    ◊ Kursorganisation und Agenda
- ♦ ◊
- ♦ **Governance at Scale**
  - ♦ ◊ Schwerpunkte der Governance at Scale
    ◊ Geschäftliche und technische Herausforderungen
- ♦ ◊
- ♦ **Automatisierte Governance**
  - ♦ ◊ Multi-Account-Strategien, Leitlinien und Architektur
    ◊ Umgebungen für Agilität und Governance at Scale
    ◊ Governance mit AWS Control Tower
    ◊ Use Cases für Governance at Scale
- ♦ ◊
- ♦ **Präventive Kontrollen**
  - ♦ ◊ Herausforderungen im Enterprise-Umfeld für Entwickler
    ◊ AWS Service Catalog
    ◊ Ressourcenerstellung
    ◊ Workflows zur Bereitstellung von Accounts
    ◊ Präventive Kosten- und Sicherheitsgovernance
    ◊ Self-Service mit bestehenden IT Service Management (ITSM)-Tools
- ♦ ◊
- ♦ **Lab 1: Bereitstellung von Ressourcen für AWS Catalog**
  - ♦ ◊ Erstellen eines neuen AWS Service Catalog-Portfolios und -Produkts
    ◊ Hinzufügen einer IAM-Rolle zu einer Launch Constraint zur Einschränkung der Aktionen, die das Produkt ausführen darf
    ◊ Gewähren des Zugriffs für eine IAM-Rolle zur Ansicht von Katalogelementen
    ◊ Bereitstellung eines S3-Buckets über ein AWS Service Catalog-Produkt
- ♦ ◊
- ♦ **Detektive Kontrollen**
  - ♦ ◊ Betriebsaspekte der Governance at Scale
    ◊ Ressourcenmonitoring
    ◊ Konfigurationsregeln für Audits
    ◊ Betriebliche Einblicke
    ◊ Remediation
    ◊ Bereinigung von Account
- ♦ ◊
- ♦ **Lab 2: Compliance- und Sicherheitsautomatisierung mit AWS Config**
  - ♦ ◊ Anwendung verwalteter Regeln (Managed Rules) mit AWS Config auf ausgewählte Ressourcen
    ◊ Automatisierung von Remediation basierend auf AWS Config-Regeln
    ◊ Untersuchung des AWS Config Dashboards und Überprüfung der Ressourcen- und Regelkonformität
- ♦ ◊
- ♦ **Lab 3: Maßnahmen mit AWS Systems Manager umsetzen**
  - ♦ ◊ Erstellen von Resource Groups für verschiedene Ressourcen basierend auf gemeinsamen Anforderungen
    ◊ Durchführung automatisierter Maßnahmen auf Ziel-Resource Groups
- ♦ ◊
- ♦ **Ressourcen**
  - ♦ ◊ Weitere Ressourcen zur Security Governance at Scale erkunden
  - ♦ ◊