

## **CL460 Security Aspects in the Implementation of IaC**

### **Kurzbeschreibung:**

Security-Experten mit technischem Verständnis, DevOps Engineers mit Security-Interesse sowie Cloud-Experten auf Associate Level erhalten eine praxisnahe Einführung in Sicherheitsaspekte bei Infrastructure as Code. Vermittelt werden der Einsatz von CI/CD-Tools wie CodePipelines und Terraform, Sicherheitsrichtlinien und Compliance-Vorgaben sowie Best Practices für sichere Pipelines. Praxisbeispiele und Fallstudien runden das Training ab.

### **Zielgruppe:**

Der Kurs **CL460 Security Aspects in the Implementation of IaC** richtet sich an:

- Security Expert mit technischem Verständnis
- DevOps Engineers mit Security Interesse / Background
- Cloud Experten im Associate Level

### **Voraussetzungen:**

Um den Inhalten und dem Lerntempo des Kurses **CL460 Security Aspects in the Implementation of IaC** gut folgen zu können, sind folgende Voraussetzungen notwendig:

- Fortgeschrittene Kenntnisse über CI/CD (Tools), Git, CLI, yaml
- Gute Cloud-Kenntnisse in AWS oder Azure, IDEs (bspw. vsCode)
- Allgemeine Sicherheitsgrundkenntnisse (Zertifikate, Schlüssel, Secrets Management)

Alternativ empfehlen wir vorab den Besuch des Trainings: [CL450 DevOps CI/CD Pipeline](#)

### **Sonstiges:**

**Dauer:** 2 Tage

**Preis:** 1690 Euro plus Mwst.

### **Ziele:**

- In den Grundlagen ist es Ziel, ein Basisverständnis von Terraform zu erhalten und eine VM zu deployen
- Sicherheitskritische Bestandteile sollen erkannt und bewertet werden
- Für sicheren Code werden Prozesse skizziert und diskutiert
- Probleme und Herausforderungen werden anhand Best-Practices diskutiert und Hilfe zur Selbsthilfe geben

## Inhalte/Agenda:

- ◆ **Grundlagen**
  - ◆     ◊ Was ist IaC?
    - ◊ Vor- und Nachteile
    - ◊ Design Prinzipien
    - ◊ Terraform Prozesse, Provider und Module
    - ◊ Konfigurationsmanagement
    - ◊ Speicherung und Versionierung von IaC
    - ◊ Beispiele, Showcases und Übungen
  - ◆     ◊
- ◆ **Design**
  - ◆     ◊ Prozesse und Richtlinien
    - ◊ Speicherung von sensitiven Informationen
    - ◊ Key Rotation
    - ◊ Identity Management
    - ◊ Beispiele, Showcases und Übungen
  - ◆     ◊
- ◆ **Automatisierung**
  - ◆     ◊ Unterstützung von Generativer KI
  - ◆     ◊ Anwendungs- vs. Infrastrukturkonfiguration
  - ◆     ◊ Execution Environment
  - ◆     ◊ Dokumentation
  - ◆     ◊ Statefull vs. Stateless Umgebungen
  - ◆     ◊ Secrets Handling
  - ◆     ◊ Beispiele, Showcases und Übungen
- ◆ **Best Practices**
  - ◆     ◊ Beispiele und Showcases
  - ◆     ◊ OWASP Top 10
  - ◆     ◊ Hilfreiche Tools und weiterführende Informationen