# Security Engineering on AWS

**Sorgen Sie durch dieses AWS Training für mehr Sicherheit und Kontrolle über Ihre Daten und Systeme in der Cloud.**

| | | |
|---|---|---|
| Seminar | 12 Termine verfügbar | Teilnahmebescheinigung |
| Präsenz / Virtual Classroom | 24 Unterrichtseinheiten | Online durchführbar |

Seminarnummer: 26009 | Herstellernummer: AWS-SECE

Stand: 12.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/26009

Sicherheit ist ein wichtiges Thema – sowohl für bestehende Cloud-Kunden als auch für Unternehmen, die eine Cloud-Einführung in Betracht ziehen. Die Zunahme von Cyberangriffen und Datenlecks beschäftigt viele Fachleute in der Branche. Der Kurs **Security Engineering on AWS** greift diese Bedenken auf, indem er Ihnen hilft, Amazon Web Services (AWS) sicher zu nutzen und zu entwickeln.

In diesem Kurs lernen Sie, wie man Identitäten und Rollen verwaltet, Konten einrichtet und verwaltet sowie API-Aktivitäten auf Unregelmäßigkeiten überwacht. Außerdem erfahren Sie, wie Sie Daten, die in AWS gespeichert sind, schützen können.

Der Kurs zeigt, wie Sie Protokolle (Logs) generieren, sammeln und überwachen können, um Sicherheitsvorfälle zu erkennen. Abschließend lernen Sie, wie Sicherheitsvorfälle mithilfe von AWS-Services erkannt und untersucht werden können.

If you would like to take this course in English, you can find more information and register here: Security Engineering on AWS (training in English).

## Nutzen

In diesem Kurs lernen Sie:

- Die AWS-Cloud-Sicherheit anhand des CIA-Prinzips (Vertraulichkeit, Integrität, Verfügbarkeit) zu verstehen
- Authentifizierung und Autorisierung mit IAM zu erstellen und zu analysieren
- Konten in AWS mit den passenden AWS-Services zu verwalten und bereitzustellen
- Möglichkeiten zur Geheimnisverwaltung (Secrets Management) mit AWS-Services zu identifizieren

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Sensible Informationen zu überwachen und Daten durch Verschlüsselung und Zugriffskontrollen zu schützen
- AWS-Services zu identifizieren, die Schutz vor externen Angriffen bieten
- Protokolle zu überwachen, zu generieren und zu sammeln
- Indikatoren für Sicherheitsvorfälle zu erkennen
- Bedrohungen zu untersuchen und mit AWS-Services geeignete Gegenmaßnahmen zu ergreifen

## Zielgruppe

Dieser Kurs richtet sich an:

- Security Engineers (Sicherheitsingenieure)
- Security Architects (Sicherheitsarchitekten)
- Cloud Architects (Cloud-Architekten)
- Cloud Operators, die in allen globalen Segmenten tätig sind

## Voraussetzungen

Für die Teilnahme an diesem Kurs empfehlen wir:

- Abschluss der folgenden Kurse:
  - AWS Security Essentials.
  - Architecting on AWS. / Architecting on AWS (training in English)
- Grundkenntnisse in IT-Sicherheitspraktiken und Infrastrukturkonzepten
- Vertrautheit mit der AWS-Cloud

## Inhalte des Seminars

**Tag 1**

**Modul 1: Sicherheitsüberblick und Wiederholung**

- Sicherheit in der AWS-Cloud erklären
- Das Shared Responsibility Model von AWS erklären
- IAM, Datenschutz sowie Bedrohungserkennung und -reaktion zusammenfassen
- Die verschiedenen Möglichkeiten zur Interaktion mit AWS über Konsole, CLI und SDKs nennen
- Die Nutzung von Multi-Factor Authentication (MFA) für zusätzlichen Schutz beschreiben
- Schutz des Root-Benutzerkontos und von Zugriffsschlüsseln erläutern

**Modul 2: Absicherung der Einstiegspunkte in AWS**

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Die Nutzung von Multi-Factor Authentication (MFA) für zusätzlichen Schutz beschreiben
- Schutz des Root-Benutzerkontos und von Zugriffsschlüsseln beschreiben
- IAM-Richtlinien, Rollen, Richtlinienkomponenten und Berechtigungsgrenzen beschreiben
- Erklären, wie API-Anfragen mit AWS CloudTrail protokolliert und die Zugriffshistorie eingesehen und analysiert werden können
- Praxislabor: Verwendung von identitäts- und ressourcenbasierten Richtlinien

**Modul 3: Kontoverwaltung und Bereitstellung in AWS**

- Verwaltung mehrerer AWS-Konten mit AWS Organizations und AWS Control Tower erklären
- Implementierung von Multi-Account-Umgebungen mit AWS Control Tower erläutern
- Die Nutzung von Identitätsanbietern und Brokern zum Zugriff auf AWS-Dienste demonstrieren
- Einsatz von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und AWS Directory Service erklären
- Verwaltung des Zugriffs von Domänenbenutzern mit Directory Service und IAM Identity Center demonstrieren
- Praxislabor: Verwaltung des Zugriffs von Domänenbenutzern mit dem AWS Directory Service

**Tag 2**

**Modul 4: Geheimnisverwaltung in AWS**

- Funktionen von AWS KMS, CloudHSM, AWS Certificate Manager (ACM) und AWS Secrets Manager beschreiben und aufzählen
- Erstellen eines Multi-Region-KMS-Schlüssels demonstrieren
- Verschlüsselung eines Secrets in AWS Secrets Manager mit einem AWS KMS-Schlüssel demonstrieren
- Nutzung eines verschlüsselten Secrets zur Verbindung mit einer Amazon RDS-Datenbank in mehreren Regionen zeigen
- Praxislabor: Lab 3 – Verwendung von AWS KMS zur Verschlüsselung von Secrets in Secrets Manager

**Modul 5: Datensicherheit**

- Überwachung von Daten auf sensible Informationen mit Amazon Macie
- Schutz ruhender Daten durch Verschlüsselung und Zugriffskontrollen beschreiben
- AWS-Dienste zur Datenreplikation für Schutz identifizieren
- Möglichkeiten zum Schutz archivierter Daten ermitteln
- Praxislabor: Lab 4 – Datensicherheit in Amazon S3

**Modul 6: Schutz der Infrastruktur am Rand (Edge Protection)**

- AWS-Funktionen zum Aufbau sicherer Infrastrukturen beschreiben
- AWS-Dienste zur Schaffung von Resilienz während eines Angriffs beschreiben

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Dienste identifizieren, die Arbeitslasten vor externen Bedrohungen schützen
- Unterschiede zwischen AWS Shield und AWS Shield Advanced vergleichen
- Erklären, wie zentrale Bereitstellung über AWS Firewall Manager die Sicherheit erhöht
- Praxislabor: Lab 5 – Verwendung von AWS WAF zur Abwehr bösartiger Zugriffe

**Tag 3**

**Modul 7: Überwachung und Protokollierung in AWS**

- Nutzen der Protokollgenerierung und -sammlung erkennen
- Amazon VPC Flow Logs zur Sicherheitsüberwachung einsetzen
- Überwachung von Abweichungen vom Grundverhalten erklären
- Amazon EventBridge Events beschreiben
- Amazon CloudWatch Metriken und Alarme beschreiben
- Optionen und Techniken zur Protokollanalyse auflisten
- Anwendungsfälle für VPC Traffic Mirroring benennen
- Praxislabor: Lab 6 – Überwachung und Reaktion auf Sicherheitsvorfälle

**Modul 8: Reaktion auf Bedrohungen**

- Vorfallarten in der Incident Response klassifizieren
- Incident-Response-Workflows verstehen
- Informationsquellen für Incident Response mit AWS-Diensten entdecken
- Vorbereitung auf Vorfälle verstehen
- Bedrohungen mit AWS-Diensten erkennen
- Sicherheitsmeldungen analysieren und darauf reagieren
- Praxislabor: Lab 7 – Incident Response

## Wichtige Hinweise

**jetzt auch online Teilnahme möglich durch unsere Virtual Classroom (VC) Lösung.** Wegen Reiseeinschränkungen können Sie nicht zu uns kommen? Wir binden Sie gerne online in das live Seminar ein. Kontaktieren Sie uns direkt damit wir dieses für Sie organisieren.

## Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/26009 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.

® TÜV, TUEV und TUV sind eingetragene Marken. Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.