Security Engineering on AWS (training in English).

Stay secure with security features in the AWS Cloud.

Seminar	8 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	24 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 26022 | Herstellernummer: AWS-SECE

Stand: 03.11.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/26022

Security is a concern for both customers in the cloud, and those considering cloud adoption. An increase in cyberattacks and data leaks remains top of mind for most industry personnel. The Security Engineering on AWS course addresses these concerns by helping you better understand how to interact and build with Amazon Web Services (AWS) in a secure way. In this course, you will learn about managing identities and roles, managing and provisioning accounts, and monitoring API activity for anomalies. You will also learn about how to protect data stored on AWS. The course explores how you can generate, collect, and monitor logs to help identify security incidents. Finally, you will review detecting and investigating security incidents with AWS services.

Nutzen

In this course, you will learn how to:

- State an understanding of AWS cloud security based on the CIA triad.
- Create and analyze authentication and authorizations with IAM.
- Manage and provision accounts on AWS with appropriate AWS services.
- Identify how to manage secrets using AWS services.
- Monitor sensitive information and protect data via encryption and access controls.
- Identify AWS services that address attacks from external sources.
- Monitor, generate, and collect logs.
- Identify indicators of security incidents.
- Identify how to investigate threats and mitigate using AWS services.

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

Zielgruppe

This course is intended for:

- Security engineers
- Security architects
- Cloud architects
- Cloud operators working accross all global segments

Voraussetzungen

We recommend that attendees of this course have:

- Completed the following courses:
  - AWS Security Essentials.
  - Architecting on AWS. / Architecting on AWS (training in English)
- Working knowledge of IT Security practices and infrastructure concepts
- Familiarity with the AWS Cloud

Inhalte des Seminars

Day 1

Module 1: Security Overview and Review

- Explain Security in the AWS Cloud.
- Explain AWS Shared Responsibility Model.
- Summarize IAM, Data Protection, and Threat Detection and Response.
- State the different ways to interact with AWS using the console, CLI, and SDKs.
- Describe how to use MFA for extra protection.
- State how to protect the root user account and access keys.

Module 2: Securing Entry Points on AWS

- Describe how to use multi-factor authentication (MFA) for extra protection.
- Describe how to protect the root user account and access keys.
- Describe IAM policies, roles, policy components, and permission boundaries.
- Explain how API requests can be logged and viewed using AWS CloudTrail and how to view and analyze access history.
- Hands-On Lab: Using Identity and Resource Based Policies.

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

Module 3: Account Management and Provisioning on AWS

- Explain how to manage multiple AWS accounts using AWS Organizations and AWS Control Tower.
- Explain how to implement multi-account environments with AWS Control Tower.
- Demonstrate the ability to use identity providers and brokers to acquire access to AWS services.
- Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service.
- Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center.
- Hands-On Lab: Managing Domain User Access with AWS Directory Service

Day 2

Module 4: Secrets Management on AWS

- Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager.
- Demonstrate how to create a multi-Region AWS KMS key. • Demonstrate how to encrypt a Secrets Manager secret with an AWS KMS key.
- Demonstrate how to use an encrypted secret to connect to an Amazon Relational Database Service (Amazon RDS) database in multiple AWS Regions
- Hands-on lab: Lab 3: Using AWS KMS to Encrypt Secrets in Secrets Manager

Module 5: Data Security

- Monitor data for sensitive information with Amaoon Macie.
- Describe how to protect data at rest through encryption and access controls.
- Identify AWS services used to replicate data for protection.
- Determine how to protect data after it has been archived.
- Hands-on lab: Lab 4: Data Security in Amazon S3

Module 6: Infrastructure Edge Protection

- Describe the AWS features used to build secure infrastructure.
- Describe the AWS services used to create resiliency during an attack.
- Identify the AWS services used to protect workloads from external threats.
- Compare the features of AWS Shield and AWS Shield Advanced.
- Explain how centralized deployment for AWS Firewall Manager can enhance security.
- Hands-on lab: Lab 5: Using AWS WAF to Mitigate Malicious Traffic

Day 3

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

Module 7: Monitoring and Collecting Logs on AWS

- Identify the value of generating and collecting logs.
- Use Amazon Virtual Private Cloud (Amazon VPC) Flow Logs to monitor for security events.
- Explain how to monitor for baseline deviations.
- Describe Amazon EventBridge events.
- Describe Amazon CloudWatch metrics and alarms.
- List log analysis options and available techniques.
- Identify use cases for using virtual private cloud (VPC) Traffic Mirroring.
- Hands-on lab: Lab 6: Monitoring for and Responding to Security Incidents

Module 8: Responding to Threats

- Classify incident types in incident response.
- Understand incident response workflows.
- Discover sources of information for incident response using AWS services.
- Understand how to prepare for incidents.
- Detect threats using AWS services.
- Analyze and respond to security findings.
- Hands-on lab: Lab 7: Incident Response

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/26022 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- 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.