Security Engineering on AWS with AWS Jam (AWSSO-AWS-JAM)

ID AWSSO-AWS-JAM **Preis** CHF 3'175.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

Dieser Kurs richtet sich an:

- Sicherheitsingenieure
- Sicherheitsarchitekten
- Cloud-Architekten
- Cloud-Betreiber, die in allen globalen Segmenten tätig sind.

Voraussetzungen

Wir empfehlen, dass die Teilnehmer dieses Kurses folgende Voraussetzungen erfüllen:

- Abgeschlossenes Studium der folgenden Kurse:
  - AWS Security Essentials (SEC-ESS) oder
  - AWS Security Fundamentals (Zweite Ausgabe) (digital) und
  - Architecting on AWS (AWSA)
- Kenntnisse von IT-Sicherheitspraktiken und Infrastrukturkonzepten.
- Vertrautheit mit der AWS-Cloud.

Kursziele

In diesem Kurs werden Sie lernen:

- Nennen Sie ein Verständnis der AWS-Cloud-Sicherheit auf der Grundlage der CIA-Trias.
- Erstellen und analysieren Sie Authentifizierungen und Berechtigungen mit IAM.
- Verwalten und Bereitstellen von Konten auf AWS mit den entsprechenden AWS-Diensten.
- Erkennen, wie man Geheimnisse mit AWS-Services verwaltet.
- Überwachen Sie sensible Informationen und schützen Sie Daten durch Verschlüsselung und Zugriffskontrollen.
- Identifizieren Sie AWS-Services, die Angriffe von externen Quellen abwehren.
- Überwachen, Erstellen und Sammeln von Protokollen.
- Identifizierung von Indikatoren für Sicherheitsvorfälle.
- Erkennen, wie man Bedrohungen untersucht und mithilfe von AWS-Services entschärft.

Kursinhalt

Modul 1: Überblick und Überprüfung der Sicherheit

- Erklären Sie die Sicherheit in der AWS-Cloud.
- Erklären Sie das AWS-Modell der geteilten Verantwortung.
- Fassen Sie IAM, Datenschutz und Bedrohungserkennung und -reaktion zusammen.
- Nennen Sie die verschiedenen Möglichkeiten der Interaktion mit AWS über die Konsole, CLI und SDKs.
- Beschreiben Sie, wie Sie MFA für zusätzlichen Schutz verwenden können.
- Geben Sie an, wie das Root-Benutzerkonto und die Zugangsschlüssel geschützt werden können.

Modul 2: Sichern von Einstiegspunkten auf AWS

- Beschreiben Sie, wie Sie die Multi-Faktor-Authentifizierung (MFA) für zusätzlichen Schutz nutzen können.
- Beschreiben Sie, wie Sie das Root-Benutzerkonto und die Zugriffsschlüssel schützen können.
- Beschreiben Sie IAM-Richtlinien, Rollen, Richtlinienkomponenten und Berechtigungsgrenzen.
- Erläutern Sie, wie API-Anfragen mit AWS CloudTrail protokolliert und eingesehen werden können und wie der Zugriffsverlauf eingesehen und analysiert werden kann.
- Praktische Übung: Verwendung von identitäts- und ressourcenbasierten Policies.

Modul 3: Kontoverwaltung und Bereitstellung auf AWS

- Erklären Sie, wie Sie mehrere AWS-Konten mit AWS Organizations und AWS Control Tower verwalten.
- Erklären Sie, wie Sie Umgebungen mit mehreren Konten mit AWS Control Tower implementieren.
- Demonstrieren Sie die Fähigkeit, Identitätsanbieter und Broker zu nutzen, um Zugang zu AWS-Diensten zu erhalten.
- Erklären Sie die Verwendung von AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) und AWS Directory Service.
- Demonstration der Fähigkeit zur Verwaltung des Domänenbenutzerzugriffs mit Directory Service und IAM Identity Center.
- Praktische Übung: Verwalten des Domänenbenutzerzugriffs mit AWS Directory Service

Modul 4: Verwaltung von Geheimnissen auf AWS

- Beschreiben und listen Sie die Funktionen von AWS KMS, CloudHSM, AWS Certificate Manager (ACM) und AWS Secrets Manager auf.
- Demonstrieren Sie, wie Sie einen AWS KMS-Schlüssel für mehrere Regionen erstellen.
- Demonstration der Verschlüsselung eines Secrets Manager-Geheimnisses mit einem AWS KMS-Schlüssel.
- Demonstration der Verwendung eines verschlüsselten Geheimnisses zur Verbindung mit einer Amazon Relational Database Service (Amazon RDS)-Datenbank in mehreren AWS-Regionen
- Praktische Übung: Übung 3: AWS KMS zum Verschlüsseln von Geheimnissen in Secrets Manager verwenden

Modul 5: Datensicherheit

- Überwachen Sie Daten auf sensible Informationen mit Amazon Macie.
- Beschreiben Sie, wie Sie Daten im Ruhezustand durch Verschlüsselung und Zugriffskontrollen schützen können.
- Identifizieren Sie die AWS-Services, die zur Replikation von Daten zum Schutz verwendet werden.
- Legen Sie fest, wie die Daten nach der Archivierung geschützt werden sollen.
- Praktische Übung: Übung 4: Datensicherheit in Amazon S3

Modul 6: Schutz der Infrastruktur an den Rändern

- Beschreiben Sie die AWS-Funktionen, die zum Aufbau einer sicheren Infrastruktur verwendet werden.
- Beschreiben Sie die AWS-Services, die bei einem Angriff für Ausfallsicherheit sorgen.
- Identifizieren Sie die AWS-Services, die zum Schutz von Workloads vor externen Bedrohungen verwendet werden.
- Vergleichen Sie die Funktionen von AWS Shield und AWS Shield Advanced.
- Erläutern Sie, wie die zentralisierte Bereitstellung für AWS Firewall Manager die Sicherheit verbessern kann.
- Praktische Übung: Übung 5: Verwendung von AWS WAF zur Eindämmung von bösartigem Datenverkehr

Modul 7: Überwachung und Erfassung von Protokollen auf AWS

- Erkennen Sie den Wert der Erstellung und Sammlung von Protokollen.
- Verwenden Sie Amazon Virtual Private Cloud (Amazon VPC) Flow Logs zur Überwachung von Sicherheitsereignissen.
- Erläutern Sie, wie Sie Abweichungen von der Grundlinie überwachen können.
- Beschreiben Sie Amazon EventBridge-Ereignisse.
- Beschreiben Sie die Metriken und Alarme von Amazon CloudWatch.
- Auflistung der Optionen für die Protokollanalyse und der verfügbaren Techniken.
- Identifizieren Sie Anwendungsfälle für die Verwendung von Virtual Private Cloud (VPC) Traffic Mirroring.
- Praktische Übung: Übung 6: Überwachung von und Reaktion auf Sicherheitsvorfälle

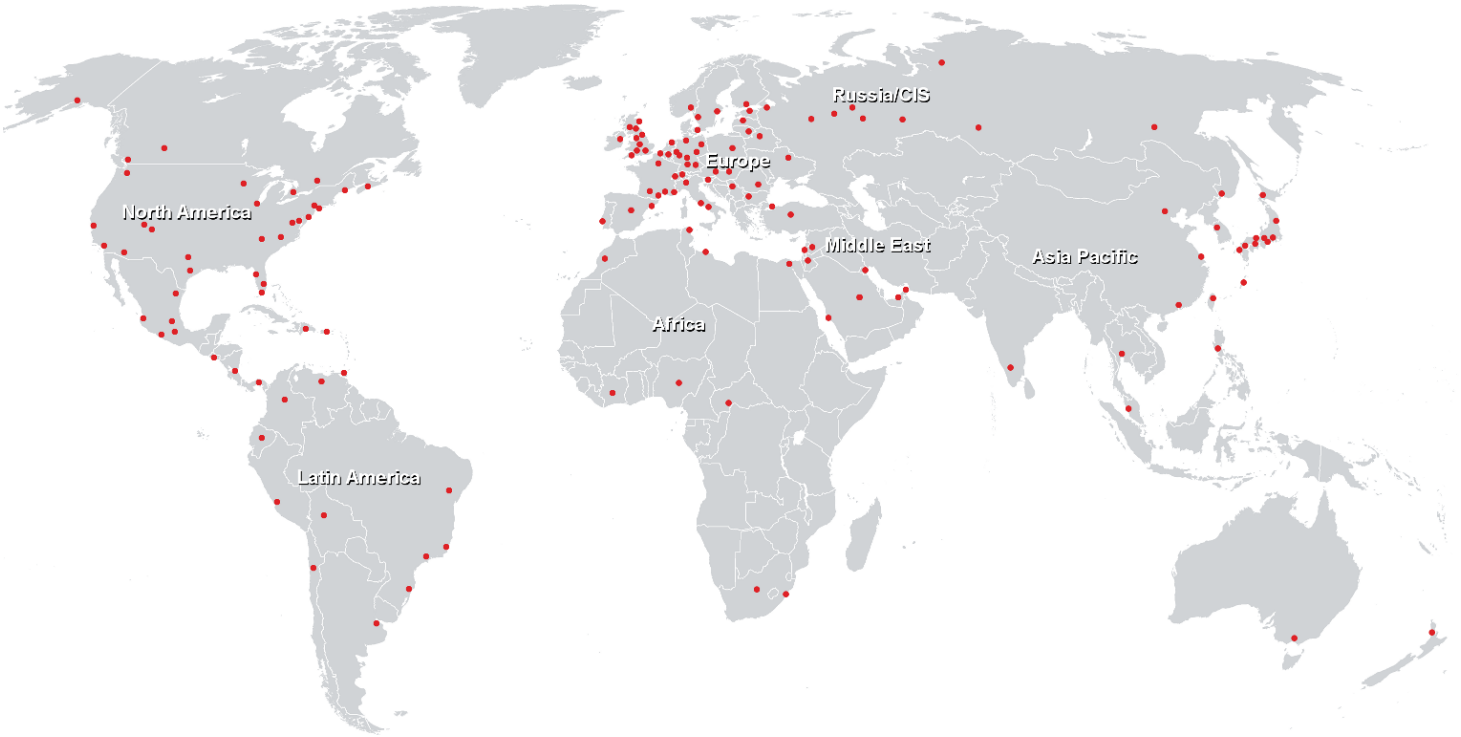
Modul 8: Reaktion auf Bedrohungen

- Klassifizierung der Vorfallstypen bei der Reaktion auf Vorfälle.
- Verstehen der Arbeitsabläufe bei der Reaktion auf Vorfälle.
- Entdecken Sie Informationsquellen für die Reaktion auf Vorfälle mit AWS-Services.
- Verstehen, wie man sich auf Zwischenfälle vorbereitet.
- Erkennen Sie Bedrohungen mithilfe von AWS-Services.
- Analyse von und Reaktion auf Sicherheitsfeststellungen.
- Praktische Übungen: Übung 7: Reaktion auf Zwischenfälle

AWS-Jam

- Nehmen Sie an teambasierten Herausforderungen in einer echten AWS-Umgebung teil.
- Messen Sie sich mit Ihren Kollegen in einer spielerischen, praktischen Lernerfahrung
- Wenden Sie Ihr Wissen aus dem Kurs auf verschiedene AWS-Services an

Weltweite Trainingscenter





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch