AWS Security Best Practices (SBP)

ID SBP **Preis** CHF 850.– (exkl. MwSt.) **Dauer** 1 Tag

Zielgruppe

Dieser Kurs richtet sich an:

Lösungsarchitekten, Cloud-Ingenieure, einschliesslich Sicherheitsingenieure, Bereitstellungs- und Implementierungsingenieure, professionelle Dienstleistungen und Cloud Center of Excellence (CCOE)

Voraussetzungen

Vor der Teilnahme an diesem Kurs sollten die Teilnehmer die folgenden Punkte absolviert haben:

- AWS-Sicherheitsgrundlagen
- AWS Security Essentials (SEC-ESS)

Kursziele

In diesem Kurs werden Sie lernen:

- Entwurf und Implementierung einer sicheren Netzinfrastruktur
- Entwurf und Implementierung von Computersicherheit
- Entwurf und Implementierung einer Protokollierungslösung

Kursinhalt

Modul 1: Überblick über die AWS-Sicherheit

- Modell der geteilten Verantwortung
- Herausforderungen für Kunden
- Rahmenwerke und Normen
- Einführung bewährter Praktiken
- Einhaltung der Vorschriften in AWS

Modul 2: Absicherung des Netzwerks

- Flexibel und sicher
- Sicherheit innerhalb der Amazon Virtual Private Cloud (Amazon VPC)
- Sicherheitsdienste
- Sicherheitslösungen von Drittanbietern

Übung 1: Kontrolle des Netzwerks

- Aufbau einer Netzinfrastruktur mit drei Sicherheitszonen.
- Implementierung der Netzwerksegmentierung mit Hilfe von Sicherheitsgruppen, Network Access Control Lists (NACLs) und öffentlichen und privaten Subnetzen.
- Überwachen Sie den Netzwerkverkehr zu Amazon Elastic Compute Cloud (EC2) Instanzen mit Hilfe von VPC Flow Logs.

Modul 4: Amazon EC2-Sicherheit

- Härten des Computers
- Amazon Elastic Block Store (EBS) Verschlüsselung
- Sichere Verwaltung und Wartung
- Erkennen von Schwachstellen
- AWS Marketplace verwenden

Übung 2: Sicherung des Startpunkts (EC2)

- Erstellen Sie ein benutzerdefiniertes Amazon Machine Image (AMI).
- Stellen Sie eine neue EC2-Instanz aus einem benutzerdefinierten AMI bereit.
- Patchen Sie eine EC2-Instanz mit AWS Systems Manager.
- Verschlüsseln Sie ein EBS-Volume.
- Verstehen Sie, wie die EBS-Verschlüsselung funktioniert und welche Auswirkungen sie auf andere Vorgänge hat.
- Verwenden Sie Sicherheitsgruppen, um den Datenverkehr zwischen EC2-Instanzen auf den verschlüsselten Datenverkehr zu beschränken.

Modul 5: Überwachung und Alarmierung

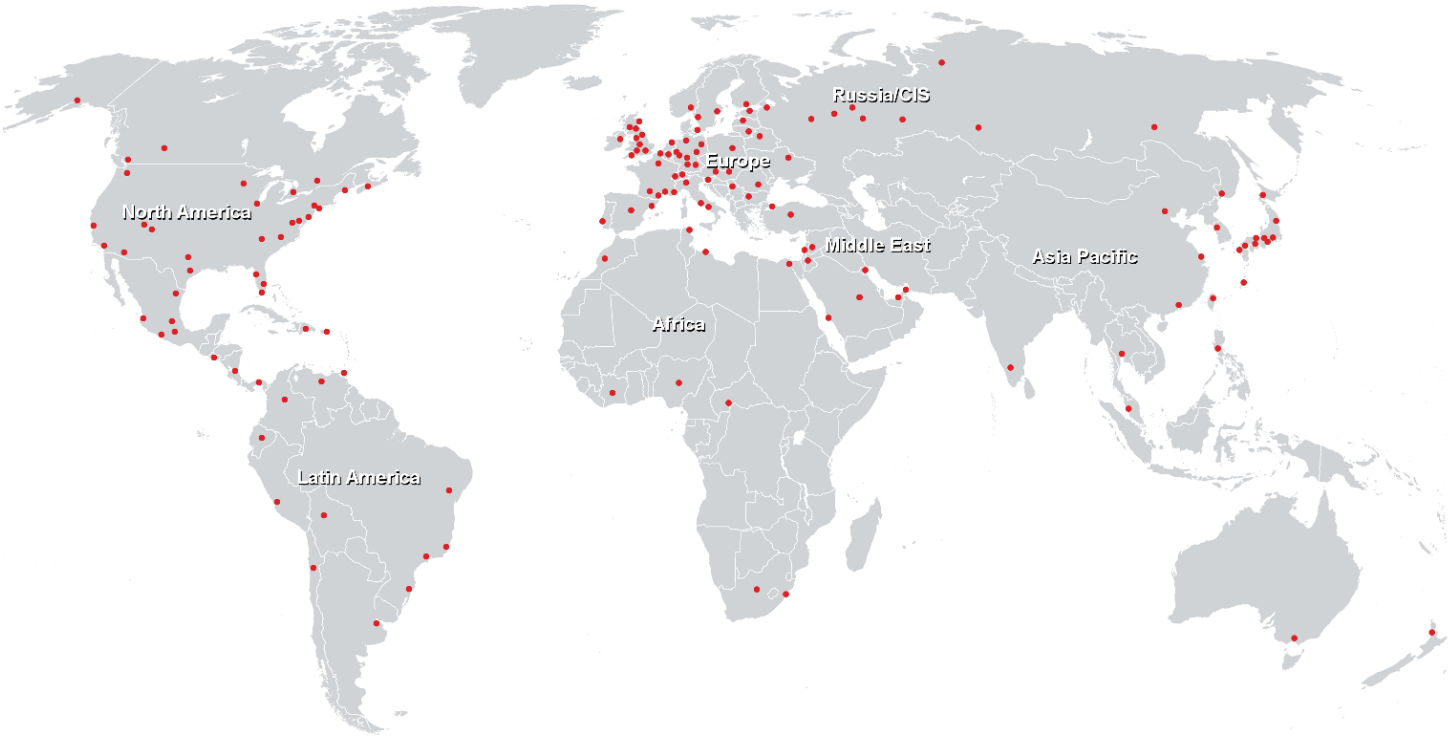
- Protokollierung des Netzwerkverkehrs
- Protokollierung des Benutzer- und API-Datenverkehrs (Application Programming Interface)
- Sichtbarkeit mit Amazon CloudWatch
- Verbessern der Überwachung und Alarmierung
- Überprüfen Ihrer AWS-Umgebung

Übung 3: Sicherheitsüberwachung

- Konfigurieren Sie eine Amazon Linux 2-Instanz, um Protokolldateien an Amazon CloudWatch zu senden.

- Erstellen Sie Amazon CloudWatch Alarme und Benachrichtigungen, um fehlgeschlagene Anmeldeversuche zu überwachen.
- Erstellen Sie Amazon CloudWatch-Alarme, um den Netzwerkverkehr durch ein Network Address Translation (NAT)-Gateway zu überwachen.

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

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

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