AWS Security Best Practices (SBP)

ID SBP **Prix** CHF 870,– (Hors Taxe) **Durée** 1 jour

A qui s'adresse cette formation

This course is intended for:

- Solutions architects, cloud engineers, including security engineers, delivery and implementation engineers, professional services, and Cloud Center of Excellence (CCOE)

Cette formation prépare à la/aux certifications

AWS Certified Advanced Networking – Specialty (ACANS)

Pré-requis

Before attending this course, participants should have completed the following:

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

Objectifs

In this course, you will learn to:

- Design and implement a secure network infrastructure
- Design and implement compute security
- Design and implement a logging solution

Contenu

Module 1: AWS Security Overview

- Shared responsibility model
- Customer challenges
- Frameworks and standards
- Establishing best practices
- Compliance in AWS

Module 2: Securing the Network

- Flexible and secure
- Security inside the Amazon Virtual Private Cloud (Amazon VPC)
- Security services
- Third-party security solutions

Lab 1: Controlling the Network

- Create a three-security zone network infrastructure.
- Implement network segmentation using security groups, Network Access Control Lists (NACLs), and public and private subnets.
- Monitor network traffic to Amazon Elastic Compute Cloud (EC2) instances using VPC flow logs.

Module 3: Amazon EC2 Security

- Compute hardening
- Amazon Elastic Block Store (EBS) encryption
- Secure management and maintenance
- Detecting vulnerabilities
- Using AWS Marketplace

Lab 2: Securing the starting point (EC2)

- Create a custom Amazon Machine Image (AMI).
- Deploy a new EC2 instance from a custom AMI.
- Patch an EC2 instance using AWS Systems Manager.
- Encrypt an EBS volume.
- Understand how EBS encryption works and how it impacts other operations.
- Use security groups to limit traffic between EC2 instances to only that which is encrypted.

Module 4: Monitoring and Alerting

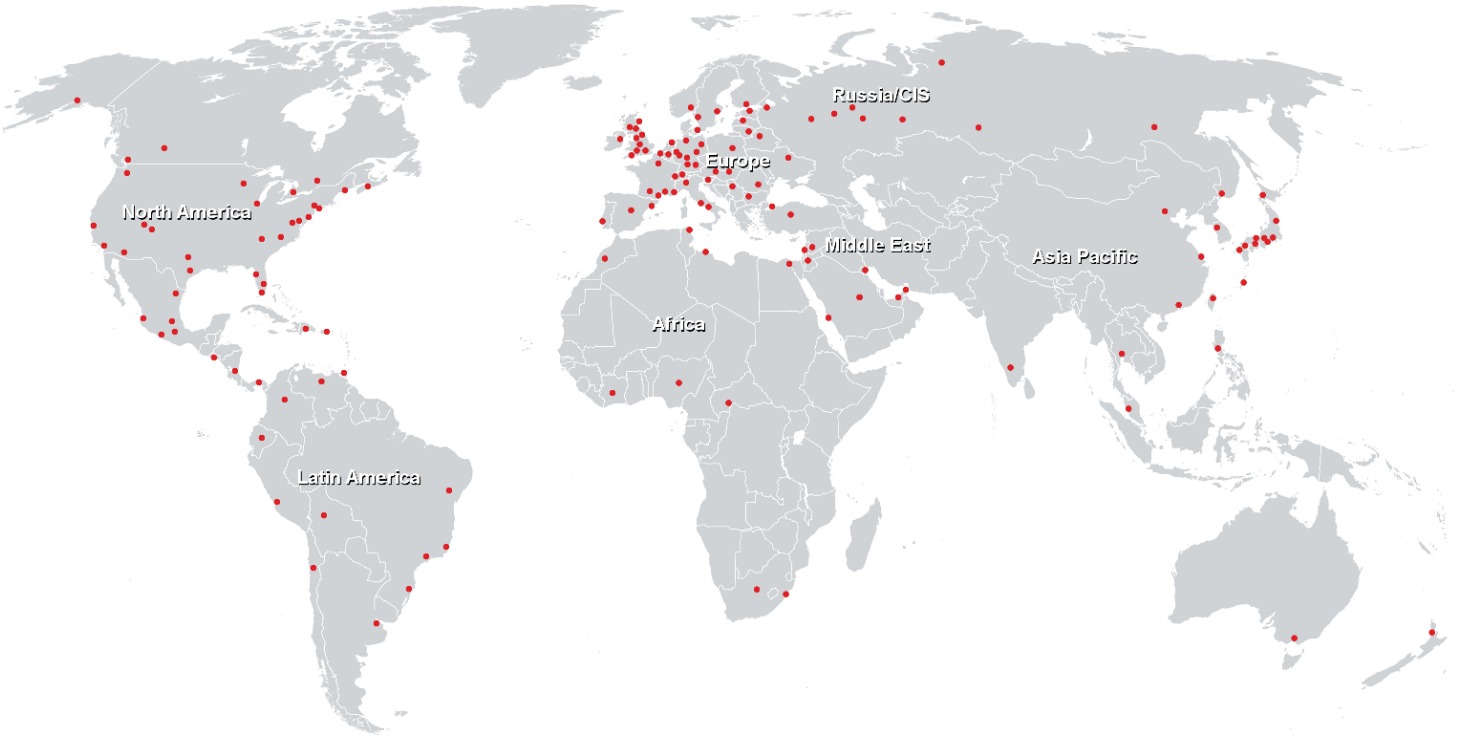
- Logging network traffic
- Logging user and Application Programming Interface (API) traffic
- Visibility with Amazon CloudWatch
- Enhancing monitoring and alerting
- Verifying your AWS environment

Lab 3: Security Monitoring

- Configure an Amazon Linux 2 instance to send log files to Amazon CloudWatch.
- Create Amazon CloudWatch alarms and notifications to monitor for failed login attempts.

- Create Amazon CloudWatch alarms to monitor network traffic through a Network Address Translation (NAT) gateway.

Centres de formation dans le monde entier



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