Security Engineering on AWS (AWSSO)

ID AW-AWSSO **Duración** 3 días

Quién debería asistir

This course is intended for:

- Security engineers
- Security architects
- Security analysts
- Security auditors
- Individuals who are responsible for governing, auditing, and testing an organization's IT infrastructure, and ensuring conformity of the infrastructure to security, risk, and compliance guidelines

Este curso es parte de las siguientes Certificaciones

AWS Certified Security - Specialty (ACSS)

Prerrequisitos

We recommend that attendees of this course have the following prerequisites:

- Attended AWS Security Fundamentals
- Experience with governance, risk, and compliance regulations and control objectives
- Working knowledge of IT security practices
- Working knowledge of IT infrastructure concepts
- Familiarity with cloud computing concepts

Objetivos del curso

Security Operations on AWS demonstrates how to efficiently use AWS security services to stay secure and compliant in the AWS cloud. The course focuses on the AWS-recommended security best practices that you can implement to enhance the security of your data and systems in the cloud. The course highlights the security features of AWS key services including compute, storage, networking, and database services. This course also refers to the common security control objectives and regulatory compliance standards and examines use cases for running regulated workloads on AWS across different verticals, globally. You will also learn how to leverage AWS services and tools for automation and continuous monitoring—taking your security operations to the next level.

This course teaches you how to:

- Assimilate and leverage the AWS shared security responsibility model.
- Mange user identity and access management in the AWS cloud.
- Use AWS security services such as AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM, and AWS Trusted Advisor.
- Implement better security controls for your resources in the AWS cloud.
- Manage and audit your AWS resources from a security perspective.
- Monitor and log access and usage of AWS compute, storage, networking, and database services.
- Assimilate and leverage the AWS shared compliance responsibility model.
- Identify AWS services and tools to help automate, monitor, and manage security operations on AWS.
- Perform security incident management in the AWS cloud.

Hands-On Activity

This course allows you to test new skills and apply knowledge to your working environment through a variety of practical exercises.

Contenido del curso

Day 1

- Introduction to Cloud Security
- Security of the AWS Cloud
- Cloud Aware Governance and Compliance
- Identity and Access Management

Day 2

- Securing AWS Infrastructure Services
- Securing AWS Container Services
- Securing AWS Abstracted Services
- Using AWS Security Services

Day 3

- Data Protection in the AWS Cloud
- Building Compliant Workloads on AWS—Case Study
- Security Incident Management in the Cloud

Esquema Detallado del Curso

Day 1

- Introduction to Cloud Security
- Security of the AWS Cloud
- Cloud Aware Governance and Compliance
- Identity and Access Management

Day 2

- Securing AWS Infrastructure Services
- Securing AWS Container Services
- Securing AWS Abstracted Services
- Using AWS Security Services

Day 3

- Data Protection in the AWS Cloud
- Building Compliant Workloads on AWS—Case Study
- Security Incident Management in the Cloud

Centros de Entrenamiento Mundial