# AWS Certified Security - Specialty

```
Course#:aws-css-b
Duration:4 Days
Price:3399.98
```

## Course Description

This track includes:

Security Engineering on AWS - 3 Days
AWS Certification Readiness Workshop - Security - 0.5 Day

This course demonstrates how to efficiently use AWS security services to stay secure in the AWS Cloud. The course focuses on the security practices that AWS recommends for enhancing 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. You will also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents.

The AWS Certified Security Specialty exam validates technical skills and experience in securing and hardening workloads and architectures on the AWS platform. Attendees with two or more years of hands-on experience designing and deploying cloud architecture on AWS should join this 2-hour, course to learn how to prepare and succeed in the exam.

## Objectives

 An understanding of specialized data classifications and AWS data protection mechanisms.
 An understanding of data encryption methods and AWS mechanisms to implement them.
 An understanding of secure Internet protocols and AWS mechanisms to implement them.
 A working knowledge of AWS security services and features of services to provide a secure production environment.
 Competency gained from two or more years of production deployment experience using AWS security services and features.
 Ability to make tradeoff decisions with regard to cost, security, and deployment complexity given a

set of application requirements.
 An understanding of security operations and risk.


## Audience

Individuals who perform a security role with at least two years of hands-on experience securing AWS workloads.

## Prerequisites

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


 AWS Cloud Practitioner
 AWS Security Fundamentals
 Architecting on AWS
 Working knowledge of IT security practices and infrastructure concepts Familiarity with cloud computing concepts


## Content

Security Engineering on AWS


Day 1


 Entry points on AWS
 Security considerations for Web Application environments
 Securing network communications inside the Amazon VPC
 Application security with incident response


Day 2


 Data security with incident response
 Security considerations for a hybrid environment
 AWS monitoring and log collecting
 Processing logs on AWS

Protecting against threats outside of the Amazon VPC

Day 3

Account management on AWS
Security considerations for a serverless environment
Secrets management on AWS
Automating security and incident response on AWS
Threat detection and sensitive data monitoring

AWS Certification Readiness Workshop - Security