

AWS Security Essentials

Duration
1 Day

Delivery Methods
VILT, Private Group



This course covers fundamental AWS cloud security concepts, including AWS access control, data encryption methods, and how network access to your AWS infrastructure can be secured. Based on the AWS Shared Security Model, you learn where you are responsible for implementing security in the AWS Cloud and what security-oriented services are available to you and why and how the security services can help meet the security needs of your organization.

Who Should Attend

Security IT business-level professionals interested in cloud security practices Security professionals with minimal to no working knowledge of AWS

Course Objectives

- Assimilate Identify security benefits and responsibilities of using the AWS Cloud
- Describe the access control and management features of AWS
- Explain the available methods for providing encryption of data in transit and data at rest when storing your data in AWS.
- Describe how to secure network access to your AWS resources
- Determine which AWS services can be used for monitoring and incident response

Agenda

1 - SECURITY ON AWS

- Security design principles in the AWS Cloud
- AWS Shared Responsibility Model

2 - SECURITY OF THE CLOUD

- AWS Global Infrastructure
- Data center security
- Compliance and governance

3 - SECURITY IN THE CLOUD – PART 1

- Identity and access management
- Data protection essentials
- Lab 01 – Introduction to security policies

4 - SECURITY IN THE CLOUD – PART 2

- Securing your infrastructure
- Monitoring and detective controls
- Lab 02 – Securing VPC resources with Security Groups

5 - SECURITY IN THE CLOUD – PART 3

- DDoS mitigation
- Incident response essentials
- Lab 03 – Remediating issues with AWS Config Conformance Packs

6 - COURSE WRAP UP

- AWS Well-Architected tool overview
- Next Steps