Security Engineering on AWS

Duration: 3 Days **Course Code: GK3338** **Version: 2**

Overview:

Security Engineering 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.

Target Audience:

This course is intended for: Security engineersSecurity architectsSecurity analystsSecurity auditorsIndividuals 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

Objectives:

- This course teaches you how to:
- Assimilate and leverage the AWS shared security responsibility model.
- Manage 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.

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

Content:

Day 1

- Module 1: Introduction to Cloud Security
- Module 2: Cloud Aware Governance and Compliance
- Module 3: Identity and Access Management
- Lab 1: Using AWS IAM
- Module 4: Securing AWS Infrastructure Services - Part 1
- Lab 2: Creating a virtual private cloud

Day 2

- Module 5: Securing AWS Infrastructure Services - Part 2
- Module 6: Securing AWS Container Services - Part 1
- Module 6: Securing AWS Container Services - Part 2
- Lab 3: Using RDS security groups
- Module 7: Securing AWS Abstracted Services
- Lab 4: Securing Amazon S3 buckets
- Module 8: Using AWS Security Services - Part 1
- Lab 5: Capturing logs

Day 3

- Module 9: Using AWS Security Products - Part 2
- Lab 6: Using AWS Config
- Lab 7: Using AWS Service Catalog
- Module 10: Data Protection in the AWS Cloud
- Module 11: Building Compliant Workloads on AWS - Case Studies
- Module 12: Security Incident Management in the Cloud

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/