Security Engineering on AWS

Duration	Delivery Methods
3 Days	VILT, Private Group

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.

Who Should Attend

This course is intended for security engineers, security architects, and information security professionals.

Course Objectives

- Identify security benefits and responsibilities of using the AWS Cloud
- Build secure application infrastructures
- Protect applications and data from common security threats
- Perform and automate security checks
- Configure authentication and permissions for applications and resources
- Monitor AWS resources and respond to incidents
- Capture and process logs
- Create and configure automated and repeatable deployments with tools such as AMIs and AWS CloudFormation

Agenda

1 - SECURITY ON AWS

- Security in the AWS cloud
- AWS Shared Responsibility Model
- Incident response overview
- DevOps with Security Engineering

2 - IDENTIFYING ENTRY POINTS ON AWS

- Identify the different ways to access the AWS platform
- Understanding IAM policies
- IAM Permissions Boundary
- IAM Access Analyzer
- Multi-factor authentication
- AWS CloudTrail

3 - SECURITY CONSIDERATIONS: WEB APPLICATION ENVIRONMENTS

- Threats in a three-tier architecture
- Common threats: user access
- Common threats: data access
- AWS Trusted Advisor

4 - APPLICATION SECURITY

- Amazon Machine Images
- Amazon Inspector
- AWS Systems Manager

5 - DATA SECURITY

- Data protection strategies
- Encryption on AWS
- Protecting data at rest with Amazon S3, Amazon RDS, Amazon DynamoDB
- Protecting archived data with Amazon S3 Glacier
- Amazon S3 Access Analyzer
- Amazon S3 Access Points

6 - SECURING NETWORK COMMUNICATIONS

- Amazon VPC security considerations
- Amazon VPC Traffic Mirroring
- Responding to compromised instances
- Elastic Load Balancing
- AWS Certificate Manager

7 - MONITORING AND COLLECTING LOGS ON AWS

- Amazon CloudWatch and CloudWatch Logs
- AWS Config
- Amazon Macie
- Amazon VPC Flow Logs
- Amazon S3 Server Access Logs
- ELB Access Logs

8 - PROCESSING LOGS ON AWS

- Amazon Kinesis
- Amazon Athena

9 - SECURITY CONSIDERATIONS: HYBRID ENVIRONMENTS

- AWS Site-to-Site and Client VPN connections
- AWS Direct Connect
- AWS Transit Gateway

10 - OUT-OF-REGION PROTECTION

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS Shield
- AWS Firewall Manager
- DDoS mitigation on AWS

11 - SECURITY CONSIDERATIONS: SERVERLESS ENVIRONMENTS

- Amazon Cognito
- Amazon API Gateway
- AWS Lambda

12 - THREAT DETECTION AND INVESTIGATION

- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective

13 - SECRETS MANAGEMENT ON AWS

- AWS KMS
- AWS CloudHSM
- AWS Secrets Manager

14 - AUTOMATION AND SECURITY BY DESIGN

- AWS CloudFormation
- AWS Service Catalog

15 - ACCOUNT MANAGEMENT AND PROVISIONING ON AWS

- AWS Organizations
- AWS Control Tower
- AWS SSO
- AWS Directory Service