INFOSECTRAIN
Educate. Excel. Empower.

AWS Combo Course

1. Architecture Foundation
2. Security Speciality

Course Highlights

- 60-Hour LIVE Instructor-led Training
- Live Demos on 30+ AWS Services
- Real-time Industry Use Cases
- Simulation Exam & Mock Test
- 3 Capstone Projects
- Interactive Flashcards
- Telegram Group for Exam Support
- Access to Recorded Sessions
- Career Guidance & Mentorship

About Course

This program has been specifically developed to provide you with a comprehensive knowledge of the AWS Security Architecture. It aims to empower you with the skills necessary to design, deploy, and manage security infrastructure on the AWS Cloud Platform. Starting from the basics of cloud computing, the program covers the essential AWS services architecture, particularly AWS Security. By participating in this program, you will gain the expertise needed to build and secure your organization's AWS infrastructure. The content is presented in a straightforward and professional manner, ensuring a clear understanding of the concepts and principles involved.

Course Objectives

By the end of this training program, participants will be able to:

- Understand the security controls for AWS environments and workloads.
- Understand security logging and monitoring capabilities.
- Able to design and implement Identity and Access Management architecture.
- Learn Encryption and Key Management for DAR and DIT.
- Manage Data retention and lifecycle management.
- Multi-account governance and organizational compliance.
- Threat detection and Incident response strategies.
- Vulnerability Management and Security Automation.
- Demonstrate your skills and working experience on AWS services.
- Learn the authentication of technical expertise to design, deploy and operate AWS applications.

Target Audience

The training is ideal for:

- Candidates with an understanding of IT security and Cybersecurity concepts
- Professionals working as Solution Architects
- Those who are working in cloud computing and security domains
- Those who want to build their career in AWS Security Architecting
- Anyone interested in gaining the AWS Security Speciality Certification
- Anyone wishing to enhance deep security knowledge related to AWS

Pre-requisites

- Knowledge of IT/Cyber Security concepts
- 3+ years of IT experience in job roles related to System Administration
- Security, Network Administrators, Operations/DevOps Engineers, etc
- Basic understanding of Virtualization fundamentals and Virtualization concepts
- 1+ years of experience in IT security domains
- Basic understanding of networking and OS concepts

Course Content

AWS Architecture Foundation

Cloud Computing Fundamentals

- ✓ Cloud Computing Concepts
- ✓ Service and Deployment models
- ✓ Shared Responsibility Model
- ✓ Virtualization Concepts
- ✓ Architecture and Security Concepts

Compute

- ✓ AWS EC2
- ✓ Amazon Lightsail
- ✓ AWS Elastic Beanstalk
  - → AWS App

Serverless

- ✓ AWS Lambda

Storage

- ✓ AWS Backup
- ✓ Amazon Elastic Block Store (Amazon EBS)
- ✓ Amazon Elastic File System (Amazon EFS)
- ✓ Amazon FSx
- ✓ Amazon S3
- ✓ Amazon S3 Glacier

Database

- Amazon RDS
- Amazon Elasticache
    - AWS DynamoDB

Container Services

- Amazon Elastic Container Service (ECS)
- AWS Elastic Kubernetes Service (EKS)
    - Amazon Elastic Container Registry (ECR)

Networking and Content Delivery

- Amazon CloudFront
- Elastic Load Balancing (ELB)
- AWS Global Accelerator
- Amazon Route 53
- Amazon VPC

Other Networking and Content Delivery Overview

- AWS VPN
- AWS Transit Gateway
- AWS Private Link
- AWS Direct Connect

Security, Identity, and Compliance

- AWS Artifact
- AWS Audit Manager
- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service

- ✓ AWS Firewall Manager
- ✓ Amazon GuardDuty
- ✓ AWS Identity and Access Management (IAM)
- ✓ Amazon Inspector
- ✓ AWS Key Management Service (AWS KMS)
- ✓ Amazon Macie
- ✓ AWS Network Firewall
- ✓ AWS Resource Access Manager (AWS RAM)
- ✓ AWS Secrets Manager
- ✓ AWS Security Hub
- ✓ AWS Shield
- ✓ AWS WAF
  - → IAM Identity Center

AWS Cost Management

- ✓ AWS Budgets
- ✓ AWS Cost and Usage Report
- ✓ AWS Cost Explorer
- ✓ Savings Plans

Analytics

- ✓ Amazon Athena
  - → Amazon Kinesis

Application Integration

- ✓ Amazon EventBridge (Amazon CloudWatch Events)
  - → Amazon Simple Notification Service (Amazon SNS)

Management and Governance

- ✓ AWS CloudFormation
- ✓ AWS CloudTrail
- ✓ Amazon CloudWatch
- ✓ AWS Command Line Interface (AWS CLI)
- ✓ AWS Config
- ✓ AWS Management Console
- ✓ AWS Organizations
- ✓ AWS Systems Manager
- ✓ AWS Trusted Advisor
- ✓ Other Management and Governance Services for review
  - → AWS Control Tower
  - → AWS License Manager

Domain 1 Threat Detection and Incident Response

Design and implement an incident response plan

- ✓ Incident Response Strategy
- ✓ Roles and responsibilities in IR plan specific to cloud incidents

→ **Use case 1**: Credentials compromise

→ **Use case 2**: Compromised EC2 Instances

- ✓ Playbooks and Runbooks for IR
- ✓ AWS Specific services helpful in Incident Response
- ✓ Third-party integration concepts
- ✓ Centralize security finding with security hub

Detect security threats and anomalies by using AWS services

- ✓ Threat detection services specific to AWS
- ✓ Visualizing and Detecting anomalies and correlation techniques
- ✓ Evaluate finding from security services
- ✓ Performing queries for validating security events
- ✓ Create metrics filters and dashboards to detect Anomalous activity

Respond to compromised resources and workloads

- ✓ AWS Security IR Guide
- ✓ Automating remediation by using AWS services
- ✓ Compromised resource management
- ✓ Investigating and analyzing to conduct Root cause and log analysis
- ✓ Capturing relevant forensics data from a compromised resource

- ✓ Protecting and preserving forensic artifacts
- ✓ Post-incident recovery

Domain 2 Security Logging and Monitoring

- ✓ Design and Implement monitoring and alerting to address security events
- ✓ Key AWS services for monitoring and alerting
- ✓ Monitoring metrics and baselines
- ✓ Analyzing environments and workloads to determine monitoring
- ✓ requirements according to business and security requirements
- ✓ Setting up tools and scripts to perform regular audits

Troubleshoot security monitoring and alerting

- ✓ Configuring monitoring services and collecting event data
- ✓ Application monitoring, alerting, and visibility challenges

Design and implement a logging solution

- ✓ Key logging services and attributes
- ✓ Log destinations, Ingestion points, and lifecycle management
- ✓ Logging specific to services and applications

Troubleshoot logging solutions

- ✓ AWS services that provide data sources and logging capabilities
- ✓ Access permissions that are necessary for logging
- ✓ Identifying misconfigurations and remediations specific to logging
- ✓ Reasons for missing logs and performing remediation steps

Design a log analysis solution

- ✓ Services and tools to analyze captured logs
- ✓ Identifying patterns in logs to indicate anomalies and known threats
- ✓ Log analysis features for AWS services

- ✓ Log format and components
- ✓ Normalizing, parsing, and correlating logs

Domain 3 Infrastructure Security

Design and implement security controls for edge services

- ✓ Define edge security strategies and security features
- ✓ Select proper edge services based on anticipated threats and attacks and define proper protection mechanisms based on that
- ✓ Define layered Defense (Defense in Depth) mechanisms
- ✓ Applying restrictions based on different criteria
- ✓ Enable logging and monitoring across edge services to indicate attacks

Design and implement network security controls

- ✓ VPC security mechanisms, including Security Groups, NACLs, and Network firewall
- ✓ Traffic Mirroring and VPC Flow Logs
- ✓ VPC Security mechanisms and implement network segmentation based on security requirements
- ✓ Network traffic management and segmentation
- ✓ Inter-VPC connectivity, Traffic isolation, and VPN concepts and deployment
- ✓ Peering and Transit Gateway
- ✓ AWS Point to Site and Site to Site VPN, Direct Connect
- ✓ Continuous optimization by identifying and removing unnecessary network access

Design and implement security controls for compute workloads

- ✓ Provisioning and maintenance of EC2 instances
- ✓ Create hardened images and backups

  - ✓ Applying instance and service roles for defining permissions
  - ✓ Host-based security mechanisms
  - ✓ Vulnerability assessment using AWS Inspector
  - ✓ Passing secrets and credentials security to computing workloads

- **Troubleshoot network security**
- **Identifying, interpreting, and prioritizing network connectivity and analyzing reachability**
- **Analyze log sources to identify problems**
- **Network traffic sampling using traffic mirroring**

Domain 4 Identity and Access Management

Design, implement, and troubleshoot authentication for AWS resources

- ✓ Identity and Access Management
- ✓ Establish identity through an authentication system based on requirements
- ✓ Managed Identities, Identity federation
- ✓ AWS Identity center, IAM, and Cognito
- ✓ MFA, Conditional access, STS
- ✓ Troubleshoot authentication issues

Design, implement, and troubleshoot authorization for AWS resources

- ✓ IAM policies and types
- ✓ Policy structure and troubleshooting
- ✓ Troubleshoot authorization issues
- ✓ ABAC and RBAC strategies
- ✓ Principle of least privilege and Separation of duties
- ✓ Investigate unintended permissions, authorization, or privileges

Domain 5 Data Protection

Design and implement controls that provide confidentiality and integrity for data in transit

- ✓ Design secure connectivity between AWS and on-premises networks
- ✓ Design mechanisms to require encryption when connecting to resources
- ✓ Requiring DIT encryption for AWS API calls
- ✓ Design mechanisms to forward traffic over secure connections
- ✓ Designing cross-region networking

Design and implement controls that provide confidentiality and integrity for data at rest

- ✓ Encryption and integrity concepts
- ✓ Resource policies
- ✓ Configure services to activate encryption for data at rest and to protect data integrity by preventing modifications
- ✓ Cloud HSM and KMS

Design and implement controls to manage the data lifecycle at rest

- ✓ Lifecycle policies and configurations
- ✓ Automated life cycle management
- ✓ Establishing schedules and retention for AWS backup across AWS services

Design and implement controls to protect credentials, secrets, and cryptographic key materials

- ✓ Designing management and rotation of secrets for workloads using a secret manager
- ✓ Designing KMS key policies to limit key usage to authorized users
- ✓ Establishing mechanisms to import and remove customer-provider key material

Domain 6 Management and Security Governance

Design a strategy to centrally deploy and manage AWS accounts

- ✓ Multi-account strategies using AWS organization and Control tower
- ✓ SCPs and Policy multi-account policy enforcement
- ✓ Centralized management of security services and aggregation of findings Securing root account access

Implement a secure and consistent deployment strategy for cloud resources

- ✓ Deployment best practices with Infrastructure as a code
- ✓ Tagging and metadata
- ✓ Configure and deploy portfolios of approved AWS services
- ✓ Securely sharing resources across AWS accounts
- ✓ Visibility and control over AWS infrastructure

Evaluate compliance of AWS resources

- ✓ Data classification by using AWS services
- ✓ Define config rules for detection of non-compliant AWS resources
- ✓ Collecting and organizing evidence by using Security Hub and AWS audit manager

Identify security gaps through architectural reviews and cost analysis

- ✓ AWS cost and usage anomaly identification
- ✓ Strategies to reduce attack surfaces
- ✓ AWS well-architected framework to identify security gaps

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on