

|  |
| --- |
| **AWS Certified Security - Specialty Training Curriculum** |



|  |
| --- |
| **AWS Certified Security - Specialty** |

|  |
| --- |
| **(*AWS Certified Security - Specialty*)**   * **About Training Program:** This course has been developed to provide you with the requisite knowledge to not only pass the AWS Certified Security Specialty certification exam but also gain the hands-on experience required to become a qualified AWS security specialist working in a real-world environment. * **Training Goals:**   + You will be prepared to give AWS Certified Security Specialty Exam   + You will be able to Master the Security aspect of AWS   + Gain deep insights about Enterprise grade Security Implementation   + You will be able to detect attacks and protect the AWS infrastructure from Hackers * **About Trainer: Certified AWS Certified Security Specialty**   + He is working with an MNC and also associated with Croma Campus Private Limited as a Part Time Trainer and Project Mentor   + 07+ Years' Experience as a Corporate Trainer   + He works primarily as a Cloud Security Consultant and helps organizations to re-build their infrastructure with security in mind   + He is one of the leading instructors in the field of Cloud & Security * Architect, Design and Implement solutions with AWS Virtual Private Cloud (VPC), Elastic Compute Cloud (EC2), Elastic Load Balancer (ELB), AutoScalling, RDS, S3, CloudWatch and other AWS products * Conducted 5000+ Hours Combined Training, 100+ Corporate Batches |

1. **Incident Response**

* Given an AWS Abuse Notice, Evaluate a Suspected Compromised Instance or Exposed Access Keys
  + AWS Abuse Notification
  + Responding to AWS Abuse Notifications
  + Performing a Source Code Security Scan Using git-secrets in AWS
  + AWS Abuse Notification
* Verify that the Incident Response plan includes relevant AWS Services
  + What is Incident Response?
  + Incident Response Framework
  + Incident Response Plan
* Evaluate the Configuration of Automated Alerting and Execute Possible Remediation of Security-Related Incidents and Emerging Issues
  + Automated Alerting
  + Automated Incident Response
  + CloudTrail Automation Example
  + Enabling AWS VPC Flow Logs with Automation

1. **Logging and Monitoring**

* Design and Implement Security Monitoring and Alerting
  + S3 Events
  + CloudWatch Logs: Metric Filters and Custom Metrics
  + CloudWatch Events
  + Multi-Account: CloudWatch Event Buses
  + AWS Config
  + AWS Inspector
  + Automatic Resource Remediation with AWS Config
  + Automatic Remediation of Inspector Findings in AWS
  + Design, Implement, and Troubleshoot Monitoring and Alerting
* Troubleshoot Security Monitoring and Alerting
  + Troubleshoot CloudWatch Events
  + Troubleshooting a Detection, Alerting, and Response Workflow in AWS
* Design and Implement a Logging Solution
  + CloudTrail Logging
  + CloudWatch Logs: CloudTrail
  + CloudWatch Logs: VPC Flow Logs
  + CloudWatch Logs: Agent for EC2
  + CloudWatch Logs: DNS Query Logs
  + S3 Access Logs
  + Multi-Account: Centralized Logging
  + Design, Implement, and Troubleshoot Logging Solutions
* Troubleshoot Logging Solutions
  + Troubleshoot Logging
  + Multi-Account: Troubleshoot Logging
  + Troubleshooting CloudTrail and S3 Logging Issues in AWS

1. **Infrastructure Security**

* Design Edge Security on AWS
  + CloudFront
  + Restricting S3 to CloudFront
  + Signed URLs and Cookies
  + CloudFront Geo Restriction
  + Forcing S3 Encryption
  + S3 Cross Region Replication (CRR) - Security
  + Web Application Firewall (WAF) and AWS Shield
  + Blocking Web Traffic with WAF in AWS
* Design and Implement a Secure Network Infrastructure
  + VPC Design and Security
  + Security Groups
  + Network Access Control Lists (NACLs)
  + VPC Peering
  + VPC Endpoints
  + Serverless Security
  + NAT Gateways
  + Egress-Only Internet Gateways
  + Bastion Hosts / Jump Boxes
  + Configuring Layered Security in an AWS VPC
* Troubleshoot a Secure Network Infrastructure
  + Troubleshoot a VPC
* Design and Implement Host-based Security
  + AWS Host/Hypervisor Security (disk/memory)
  + Host Proxy Servers
  + Host-Based IDS/IPS
  + Systems Manager
  + Packet Capture on EC2
  + Install an Intrusion Prevention System (IPS) on an EC2 Instance

1. **Identity and Access Management**

* Design and Implement a Scalable Authorization and Authentication System to Access AWS Resources
  + IAM Policies
  + Users, Groups, and Roles
  + Permission Boundaries and Policy Evaluation
  + Organizations and Service Control Policies
  + Resource Policies: S3 Bucket Policies
  + Resource Policies: KMS Key Policies
  + Cross-Account Access to S3 Buckets and Objects
  + Identity Federation
  + AWS Systems Manager Parameter Store
* Troubleshoot an Authorization and Authentication System to Access AWS Resources
  + Troubleshooting Permissions Union (IAM//RESOURCE//ACL)
  + Troubleshooting Cross-Account Roles
  + Troubleshooting Identity Federation
  + Troubleshooting KMS CMK's

1. **Data Protection**

* Design and Implement Key Management and Use
  + Key Management System (KMS)
  + KMS in a Multi-Account Configuration
  + CloudHSM
* Troubleshoot Key Management
  + Troubleshooting KMS Permissions
  + KMS Limits
  + Troubleshoot KMS Key Policies
* Design and Implement a Data Encryption Solution for Data at Rest and Data in Transit
  + Data At Rest: KMS
  + Data At Rest: Server-side encryption with SSE-C
  + Data In Transit: Certificate Manager (ACM)
  + Encryption SDKs
  + Compliance Examples
  + Create and Manage SSL Certificates with AWS Certificate Manager