multisoft
Systems

AWS Certified Security - Specialty Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The AWS Certified Security - Specialty training by Multisoft Systems is designed for IT professionals who want to deepen their expertise in cloud security and achieve an advanced understanding of AWS security protocols. This specialized course covers critical areas such as data protection, identity and access management, infrastructure security, threat detection, and compliance, all tailored to AWS's environment.

Module 1: Threat Detection and Incident Response

1.1 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

1.2 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

1.3 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

Module 2: Security Logging and Monitoring

2.1 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

2.2 Troubleshoot security monitoring and alerting

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

2.3 Design and implement a logging solution

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

2.4 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

2.5 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

Module 3: Infrastructure Security

3.1 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

3.2 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

3.3 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
- ✓ Analyse log sources to identify problems
- ✓ Network traffic sampling using traffic mirroring

Module 4: Identity and Access Management

4.1 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

4.2 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

Module 5: Data Protection

5.1 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

5.2 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

5.3 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.

5.4 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.

Module 6: Management and Security Governance

6.1 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

6.2 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

6.3 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

6.4 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