AWS Certified Security – Specialty

Course Outline

Day 1

- **Module 1: Security Overview and Review**
  - Explain Security in the AWS Cloud
  - Explain AWS Shared Responsibility Model
  - Summarize IAM, Data Protection, and Threat Detection and Response
  - State the different ways to interact with AWS using the console, CLI, and SDKs
  - Describe how to use MFA for extra protection
  - State how to protect the root user account and access keys

- **Module 2: Securing Entry Points on AWS**
  - Describe how to use multi-factor authentication (MFA) for extra protection
  - Describe how to protect the root user account and access keys
  - Describe IAM policies, roles, policy components, and permission boundaries
  - Explain how API requests can be logged and viewed using AWS CloudTrail and how to view and analyze access history
  - **Hands-On Lab: Using Identity and Resource-Based Policies**

- **Module 3: Account Management and Provisioning on AWS**
  - Explain how to manage multiple AWS accounts using AWS Organizations and AWS Control Tower
  - Explain how to implement multi-account environments with AWS Control Tower
  - Demonstrate the ability to use identity providers and brokers to acquire access to AWS services
  - Explain the use of AWS IAM Identity Center (successor to AWS Single Sign-On) and AWS Directory Service
  - Demonstrate the ability to manage domain user access with Directory Service and IAM Identity Center
  - **Hands-On Lab: Managing Domain User Access with AWS Directory Service**

Day 2

- **Module 4: Secrets Management on AWS**
  - Describe and list the features of AWS KMS, CloudHSM, AWS Certificate Manager (ACM), and AWS Secrets Manager
  - Demonstrate how to create a multi-Region AWS KMS key
  - Demonstrate how to encrypt a Secrets Manager secret with an AWS KMS key
  - Demonstrate how to use an encrypted secret to connect to an Amazon RDS

database in multiple AWS Regions
    - **Hands-On Lab: Using AWS KMS to Encrypt Secrets in Secrets Manager**

- **Module 5: Data Security**
    - Monitor data for sensitive information with Amazon Macie
    - Describe how to protect data at rest through encryption and access controls
    - Identify AWS services used to replicate data for protection
    - Determine how to protect data after it has been archived
    - **Hands-On Lab: Data Security in Amazon S3**

- **Module 6: Infrastructure Edge Protection**
    - Describe the AWS features used to build secure infrastructure
    - Describe the AWS services used to create resiliency during an attack
    - Identify the AWS services used to protect workloads from external threats
    - Compare the features of AWS Shield and AWS Shield Advanced
    - Explain how centralized deployment for AWS Firewall Manager can enhance security
    - **Hands-On Lab: Using AWS WAF to Mitigate Malicious Traffic**

Day 3

- **Module 7: Monitoring and Collecting Logs on AWS**
    - Identify the value of generating and collecting logs
    - Use Amazon VPC Flow Logs to monitor for security events
    - Explain how to monitor for baseline deviations
    - Describe Amazon EventBridge events
    - Describe Amazon CloudWatch metrics and alarms
    - List log analysis options and available techniques
    - Identify use cases for using VPC Traffic Mirroring
    - **Hands-On Lab: Monitoring for and Responding to Security Incidents**

- **Module 8: Responding to Threats**
    - Classify incident types in incident response
    - Understand incident response workflows
    - Discover sources of information for incident response using AWS services
    - Understand how to prepare for incidents
    - Detect threats using AWS services
    - Analyze and respond to security findings
    - **Hands-On Lab: Incident Response**