CLOUD INTERMEDIATE 4 DAYS

AWS Certified Security Specialty

Build a strong foundation in AWS security services, architectures, and best practices to protect cloud workloads at scale. Learn how to design secure environments, manage risk, respond to incidents, and meet compliance and governance requirements across AWS platforms.

Why AWS Security?

Practical skills

Demonstrates Expertise: The certification validates the team's knowledge and skills, giving clients and partners confidence in your organization's ability to handle their security needs effectively.

Enterprise outcomes

Mitigates Security Risks: By having certified security professionals, your business can proactively identify and address potential security risks, minimizing the impact of breaches or unauthorised access.

Operational readiness

Ensures Best Security Practices: The certification equips your team with a deep understanding of AWS security best practices. They learn how to implement robust security controls, protect data, and mitigate risks, ensuring that your business operates securely and competently.

What you'll be able to do

- Gain a comprehensive understanding of AWS Security services, features, and best practices.
- Learn key security concepts and frameworks relevant to AWS.
- Develop the skills to design and implement secure architectures on the AWS platform.
- Gain knowledge and skills in identifying, assessing, and mitigating security risks on the AWS platform.
- Learn how to establish incident response plans, detect and respond to security incidents, and recover from security breaches or disruptions.
- Understand the importance of compliance and governance in AWS security.

Who this is for

- Security Professionals Cloud Architects Systems Administrators DevOps Engineers
- Compliance and Risk Management Professionals

Curriculum

01 Incident Response

- Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys
- Verify that the Incident Response plan includes relevant AWS services
- Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

02 Logging and Monitoring

- Design and implement security monitoring and alerting
- Troubleshoot security monitoring and alerting
- Design and implement a logging solution
- Troubleshoot logging solutions.

03 Infrastructure Security

- Design edge security on AWS
- Design and implement a secure network infrastructure
- Troubleshoot a secure network infrastructure
- Design and implement host-based security.

04 Identity and Access Management

- Design and implement a scalable authorization and authentication system to access AWS resources
- Troubleshoot an authorization and authentication system to access AWS resources.
- Validate configuration and confirm expected outcomes in the lab environment

05 Data Protection

- Design and implement key management and use
- Troubleshoot key management
- Design and implement a data encryption solution for data at rest and data in transit.