Security Engineering on AWS

Category: Cloud Platforms | **Vendor:** Amazon Web Services

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	AWS Certified Security – Specialty
Related Exam:	SCS-C02

Course Overview

Cybersecurity threats are escalating, and organizations need professionals who can efficiently use AWS security services to stay secure in the AWS Cloud. Security Engineering on AWS focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. This course highlights the security features of AWS key services including compute, storage, networking, and database services. You'll also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents. Through hands-on labs and real-world scenarios, you'll gain practical experience in implementing security solutions, understanding specialized data classifications and AWS data protection mechanisms, and applying security best practices. This training is designed to help you stay secure in the AWS Cloud and prepare for the AWS Certified Security – Specialty certification.

About This Course

Cybersecurity threats are escalating, and organizations need professionals who can efficiently use AWS security services to stay secure in the AWS Cloud. Security Engineering on AWS focuses on the security practices that AWS recommends for enhancing the security of your data and systems in the cloud. This course highlights the security features of AWS key services including compute, storage, networking, and database services. You'll also learn how to leverage AWS services and tools for automation, continuous monitoring and logging, and responding to security incidents. Through hands-on labs and real-world scenarios, you'll gain practical experience in implementing security solutions, understanding specialized data classifications and AWS data protection mechanisms, and applying security best practices. This training is designed to help you stay secure in the AWS Cloud and prepare for the AWS Certified Security – Specialty certification.

Who Should Attend

This course is intended for security engineers, security architects, and information security professionals.

Prerequisites & Entry Requirements

General Prerequisites:

We recommend that attendees of this course have:

- Working knowledge of IT security practices and infrastructure concepts
- Familiarity with cloud computing concepts
- Completed AWS Security Essentials and Architecting on AWS courses

Learning Outcomes

Upon successful completion of this course, participants will be able to:

Security Engineering on AWS prepares you to design, implement, and manage secure infrastructure on the AWS cloud platform. You'll learn to protect applications and data from common security threats, perform and automate security checks, and configure authentication and permissions for applications and resources. By the end of this course, you'll be able to monitor AWS resources and respond to incidents, capture and process logs, and create automated and repeatable deployments with tools such as AMIs and AWS CloudFormation. This course focuses on the security practices that AWS recommends for enhancing the security of your systems in the cloud.

Detailed Course Outline

Module 1: Introduction to Security in the AWS Cloud

- Understand the AWS Shared Responsibility Model
- Explore core cloud security principles
- Review incident response strategies in AWS
- Align DevOps processes with security engineering

Module 2: Managing Identity and Access Control

- Define and apply IAM policies, roles, and permissions boundaries
- Use IAM Access Analyzer for insight into access risks
- Implement multi-factor authentication (MFA)
- Monitor access activity with AWS CloudTrail

Module 3: Securing Web Application Environments

- Analyze threats to 3-tier application architectures
- Address common risks around user and data access
- Leverage AWS Trusted Advisor for continuous improvement

Module 4: Application Security at Scale

- Harden Amazon Machine Images (AMIs)
- Perform automated security assessments with Amazon Inspector
- Apply secure configuration management with AWS Systems Manager

Module 5: Data Protection and Encryption Best Practices

- Encrypt data in S3, RDS, DynamoDB, and Glacier
- Apply key management strategies using AWS KMS
- Use S3 Access Analyzer and Access Points for precise control

Module 6: Network Security and Traffic Protection

- Implement best practices for securing Amazon VPCs
- Use VPC Traffic Mirroring for deep packet inspection
- Respond to compromised instances
- Secure endpoints with AWS Certificate Manager and ELB

Module 7: Centralized Monitoring and Logging

- Configure CloudWatch, AWS Config, and Amazon Macie
- Enable VPC Flow Logs, ELB Logs, and S3 Server Access Logs

Module 8: Log Processing and Analysis

- Aggregate log data with Amazon Kinesis
- Analyze security events using Amazon Athena

Module 9: Securing Hybrid Cloud Architectures

- Connect environments with VPNs and Direct Connect
- Secure cross-region traffic with AWS Transit Gateway

Module 10: Building Global Resilience and DDoS Protection

- Use Route 53 and CloudFront for edge-level protection
- Defend against attacks with AWS WAF, Shield, and Firewall Manager

Module 11: Serverless Security Practices

- Control access in serverless environments with Amazon Cognito
- Secure APIs with API Gateway
- Implement least-privilege execution in AWS Lambda

Module 12: Threat Detection and Investigation

- Identify suspicious activity with Amazon GuardDuty
- Consolidate findings in AWS Security Hub
- Perform forensic analysis with Amazon Detective

Module 13: Secrets and Key Management

- Manage encryption keys using AWS KMS and CloudHSM
- Store and rotate secrets with AWS Secrets Manager

Module 14: Automating Security by Design

- Create secure, repeatable deployments with AWS CloudFormation
- Standardize infrastructure with AWS Service Catalog

Module 15: Governance and Account Management at Scale

- Manage multi-account environments with AWS Organizations
- Enforce controls using AWS Control Tower and AWS SSO
- Integrate centralized identity with AWS Directory Services

, Day 3, Day 2, Day 1

□□ Certification Path

AWS Certified Security – Specialty

Exam: SCS-C02

Skills You Will Learn:

In this course, you will:

- State an understanding of AWS cloud security based on the CIA triad.
- Create and analyze authentication and authorizations with IAM.
- Manage and provision accounts on AWS with appropriate AWS services.
- Identify how to manage secrets using AWS services.
- Monitor sensitive information and protect data via encryption and access controls.
- Identify AWS services that address attacks from external sources.
- Monitor, generate, and collect logs.
- Identify indicators of security incidents.
- Identify how to investigate threats and mitigate using AWS services.

Frequently Asked Questions

Q: What delivery options are available for Security Engineering on AWS?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Security Engineering on AWS course helps prepare you for the AWS Certified Security – Specialty certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the SCS-C02 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day Security Engineering on AWS course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Security Engineering on AWS training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Security Engineering on AWS?

Yes, we provide corporate training, dedicated training, and closed classes for Security Engineering on AWS. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Security Engineering on AWS, Security, AWSSO, Amazon Web Services, vILT

Q: Why choose Nexus Human for Security Engineering on AWS?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Security Engineering on AWS training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.