Security Specialty Exam (SCS-C02) Overview

Chandra Lingam, Compute With Cloud Inc, https://www.computewithcloud.com/

Introduction

Here are a few things you need to know to pass the exam and be an effective security engineer (which you will learn in this course!!!)

- Are you familiar with common attacks, threats, and exploits (such as OWASP Top 10, DDOS)?
- Do you know how to secure various resources in AWS?
- Do you know how to protect your data during transit and at-rest?
- How do you keep the traffic private inside your AWS environment and on-premises?
- Do you know how to detect configuration drifts, identify misconfigured resources and fix?
- Are you familiar with network-based access controls, identify based access controls?
- Are you familiar with tools that can automatically identify and report security issues?
- Are you familiar with tools that can automatically block attacks?
- Do you know what information these tools report and in what format (like ASFF - AWS Security Finding Format)?
- Do you know how to remediate the reported issues?
- How do you streamline incident response?
- How would you automate remediation?
- How do you revoke access to compromised credentials?
- How do you collect evidence?
- How do you isolate resources that are impacted?
- Are you familiar with data sources that can log activities? Do you know how to enable logging?
- Are you familiar with log destinations and the format in which the events are logged?
- How do you monitor all the regions and centralize the findings?
- How can you analyze the logged data and find the root cause?
- How do you protect your logs from tampering?
- How do you protect your data from tampering?
- How do you restore data when needed?
- How do you integrate third-party security solutions?
- How do you manage multiple accounts?
- Are you familiar with tools like CloudFormation to deploy your infrastructure?

Brief Overview (based on SCS-C02 Exam Guide)

“This exam validates an examinee’s ability to effectively demonstrate knowledge about securing the AWS platform.”

Here are some of the applied areas that you should focus

- Data Classification and Protection
- Data Encryption
- Secure Transport
- AWS Security Services

Besides, AWS expects you to have hands-on experience using AWS offerings in the security space, ability to make the cost-security-complexity tradeoff for a given requirement, and understanding security operations and risk.

This course is designed to accelerate the learning.

As a pre-requisite, I recommend that you have familiarity with the AWS environment and a certification like Cloud Practitioner or Associate level.

Let me give a brief overview of each of the above areas

Data Classification and Protection

Here the focus is on protecting against unintentional disclosure of data stored in AWS.

Enterprises typically use a three-tier classification.

For example, from the AWS data classification whitepaper,

Tier 1 – Protected Data

- Information for internal use
- Vendor bank account information
- Information for internal use only

Tier 2 – Restricted Data

- Sales and marketing data, executed contracts, receipts
- Employee HR records

Tier 3 – Highly Strategic

- Trade secret
- Pricing information
- Merger/acquisition information
- Proprietary Process
- Inventions before patent
- Public disclosure could cause severe or catastrophic legal, financial, or reputational damage.

Depending on the classification, it is essential to employ a suitable data protection mechanism.

The questions in the exam will spell out the classification details and type of protection required. You then need to pick the correct answer that meets the requirement.

Data encryption

You need a good understanding of data encryption methods and how AWS implements them.

For example, key management, symmetric encryption, asymmetric encryption, digital signing, encryption of data-at-rest, encryption of data in transit, and so forth

Secure Internet protocols

Secure communication protocols such as TLS/SSL, VPN, SSH (Linux/Unix client), SFTP, RDP (windows client),

AWS Security Services

You need to be familiar with the AWS service and its purpose, whether it simply flags suspicious events or actively defends against attacks.

AWS offers various services under Identity and Access Management, Threat Detection, Configuration drift detection, Infrastructure protection, Data protection, Incident response, etc.

A list of products is available here: https://aws.amazon.com/products/security/

Exam Details

The security specialty exam is 170 minutes long and has about 65 questions. Only 50 of the questions are graded, and 15 unscored questions in the exam are not identified.

So, you get around two and a half minutes per question.

The question format is like other AWS exams: multiple-choice or multiple responses.

In Multiple-choice questions, you need to pick one correct response from the choice given.

In multiple-response questions, you need to choose two or more correct answers out of five or more options.

So, read the question carefully; for multiple-response, it will tell you how many choices you need to pick.

In general, if you prepare well, you can quickly eliminate 50% of the choices given for a problem.

You need to use experience and knowledge to pick one of the options among the remaining choices.

There is no penalty for guessing – so don't leave any questions unanswered.

One or two questions may come from topics that you are not familiar with. AWS can place unscored items in the mix to gather data.

So, if you see a question from an unfamiliar topic, don't panic –keep calm, pick a choice that makes the most sense, and move on.

The score range is 100-1000. The passing score is **750.**

The fee for the exam is USD 300.

AWS issues a 50% off exam voucher whenever you achieve certification; you can use this voucher for future exams. So, your effective fee with a voucher is USD 150.

Domains

Reference: Security Specialty Exam Guide SCS-C02

Domain	Percentage of Examination (Change from SCS-C01)
Threat Detection and Incident Response	**14%** (from 12%)
Security Logging and Monitoring	**18%** (from 20%)
Infrastructure Security	**20%** (from 26%)
Identity and Access Management	**16%** (from 20%)

Data Protection	**18%** (from 22%)
Management and Security Governance (New)	**14%** (N/A)
Total	100%

Useful Resources:

Best Practices for Security, Identity, & Compliance
https://aws.amazon.com/architecture/security-identity-compliance/

Security Pillar - AWS Well-Architected Framework
https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

Cloud Incident Response Essentials - Plan Ahead to Improve Security
Highly recommended and crisp video, and you can skip reading the Security Incident Response Guide!

AWS re:Inforce 2022 - Cloud incident response essentials: Plan ahead to improve security (TDR205)

https://www.youtube.com/watch?v=PTtXpkNqR9I&ab_channel=AWSEvents

AWS Security Incident Response Guide
https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html

AWS Data Classification
https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification.html

SCS-C02 Exam Guide
https://d1.awsstatic.com/training-and-certification/docs-security-spec/AWS-Certified-Security-Specialty_Exam-Guide.pdf

SCS-C02 Official Practice Question Set
https://explore.skillbuilder.aws/learn/course/external/view/elearning/15222/aws-certified-security-specialty-official-practice-question-set-scs-c02-english

Pearson Whiteboard Practice (for online exam):

The online exam has a whiteboard feature. It's basically a text editor with a drawing surface. I found it difficult to draw on the whiteboard with a mouse or trackpad, so I mostly used the text editor to capture key question details and answer choices. Pearson offers a whiteboard practice tool, which is very useful for preparation.

https://home.pearsonvue.com/Standalone-pages/Whiteboard.aspx#practice-whiteboard

Exam Preparation

Step 1: Go through all the lectures in sequence and complete all the labs and quizzes. Absorb any new information. Use the course Q&A forum if you need clarification.

Step 2: Take the exam readiness videos available on the skill builder website. It has several sample questions. https://explore.skillbuilder.aws/learn/global-search/exam%20readiness

Step 3: Go through the official practice question set and assess your gaps

https://explore.skillbuilder.aws/learn/course/external/view/elearning/15222/aws-certified-security-specialty-official-practice-question-set-scs-c02-english

Step 4: Review lectures again based on the gaps

Step 5: Read the whitepapers (Security Pillar, Security Incident Response Guide)

Step 6: Appear for the Security Specialty Exam!

Learning is two-way, and I am here to help you. You can reach me through the course Q&A forum, and I am happy to hear from you and answer your questions.