CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCCS Certification Exam Guide

Description

Successful completion of the CrowdStrike Certified Cloud Specialist (CCCS) exam is required to earn the CCCS certification. This exam evaluates a candidate's knowledge, skills and abilities to perform administrative and vulnerability management tasks within the Falcon platform to mitigate and prevent risks.

A successful CrowdStrike Certified Cloud Specialist:

- Sets up and configures Falcon Cloud Security to monitor and respond to security issues
- Understands the features and services of Falcon Cloud Security
- Manages cloud account registration for an organization
- Configures cloud security policies and rules
- Manages pre-runtime and runtime protection
- Performs detection analysis
- Remediates and reports issues when necessary

CrowdStrike Certification Program

Requirements

All exam registrants must (no exceptions):

- Accept the CrowdStrike Certification Exam Agreement
- Be at least 18 years of age
- Purchase a CrowdStrike exam voucher to register for the exam

Contact your CrowdStrike Account Executive to request a quote or purchase a CrowdStrike exam voucher through Pearson.

Learning Access

It is **strongly recommended** that all exam candidates have access to CrowdStrike University and confirm they can view available learning options associated with their CrowdStrike University account.

- CrowdStrike certification-aligned courses are available to learners with an active CrowdStrike University account.
- A unique CrowdStrike University ID, training transcripts and printable certification documents are available through the CrowdStrike University learning management system.

NOTE: All exam takers can view and print their CrowdStrike certification exam score report through Pearson.

Recommended Certification Candidate Competence and Abilities

- Candidates should have at least six (6) months of experience with CrowdStrike Falcon in a production environment.
- Candidates should read English with sufficient accuracy and fluency to support comprehension. Exams are suitable for non-native English speakers.

About the Exam

Assessment Method

The CCCS exam is a 90-minute, 60-question assessment.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCCS certification exam
- Refrain from any misconduct

In the event of misconduct by the candidate, CrowdStrike may invalidate the score and consider any suspicious action a violation of the CrowdStrike Certification Exam Agreement.

When a candidate has completed the exam and the candidate's official exam score has been posted, the certification candidate may view the official exam score through Pearson.

Retake Policy

Candidates who do not pass an exam on their first attempt:

- Must wait 48 hours to retake the exam (wait time begins after the exam)
- Should review the exam objectives, training course materials and associated recommended reading listed in this document

After the second attempt, a candidate will need to wait seven (7) days for the third attempt and any subsequent attempts. Wait time begins the day after the attempt.

Candidates that want to retake the exam should consider retaking the applicable recommended course(s) and gain additional experience with the CrowdStrike Falcon platform before trying again.

Retakes beyond the fourth attempt will be considered on a case-by-case basis. CrowdStrike reserves the right to deny a retake beyond the fourth attempt. If the fourth attempt is a failure due to a technical issue, the student can reattempt the exam a fifth time.

If the student fails for a fourth time due to personal performance, they must wait 30 days and retake the recommended training indicated in the exam guide. CrowdStrike will verify that the candidate has retaken the recommended training in the exam guide and has met with the CrowdStrike Certification Manager before they are cleared to register for a fifth exam attempt.

Retaking Previously Passed Exams

Candidates will not be permitted to retake any exam they have previously passed unless directly related to a recertification requirement approved by CrowdStrike.

Beta Exams

Candidates will not be permitted to retake beta exams.

Exam Challenge

If a certification candidate believes there is an error on an exam or that specific questions on the CCCS exam are invalid, contact certification@crowdstrike.com to request an evaluation of your claim. The certification candidate must submit a claim within three (3) days of taking the exam for it to be considered. CrowdStrike will generally respond to your submission within fifteen (15) business days.

Recertification

All CrowdStrike certifications are valid for three (3) years from the date of successful completion of an exam. Recertification requires passing the most current version of the exam upon expiration of certification.

Exam Preparation

Recommended Training

CrowdStrike strongly recommends certification candidates complete the CrowdStrike Certified Cloud Specialist courses in CrowdStrike University to prepare for the CCCS exam. To learn more about these courses, view the CrowdStrike Training Catalog.

Recommended Reading

CrowdStrike strongly recommends certification candidates review the following CrowdStrike Falcon Support Documentation titles to prepare for the CCCS exam:

- Cloud Security Overview
- Cloud Security Posture Management: Cloud Asset Inventory and Visualization
- Cloud Security Posture Management: CSPM Automated Remediation
- Cloud Security Posture Management: Configuring CSPM
- Cloud Security Posture Management: Identity Analyzer
- Cloud Security Posture Management: CSPM Overview
- Cloud Security Posture Management: Monitoring CSPM Assessment Findings
- Cloud Security Posture Management: Troubleshooting Cloud Security Posture Management
- Cloud Security Posture Management: Registering Accounts
- Kubernetes and Containers: Container Security
- Kubernetes and Containers: Kubernetes Protection

Exam Scope

The following topics provide a general guideline for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam.

1. Falcon Cloud Security Features and Services
2. Cloud Account Registration
3. Cloud Security Policies and Rules
4. Pre-Runtime Protection
5. Runtime Protection
6. Findings and Detection Analysis
7. Remediating and Reporting Issues

Scope Changes

To better reflect the content of the exam and for clarity purposes, the following guidelines may change at any time without notice. Such changes may include, without limitation, adding or deleting an available CrowdStrike certification, modifying certification requirements, and making changes to recommended training courses, testing objectives, outline and exams, including, without limitation, how and when exam scores are issued. The certification candidate agrees to meet (and continue to meet) the program requirements, as amended, as a condition of obtaining and maintaining the certification.

Exam Objectives

The following subtopics and learning objectives provide further guidance on the content and purpose of the exam:

1. Falcon Cloud Security Features and Services

1.1 Explain the benefits of CrowdStrike's cloud security products and services — including cloud security posture management (CSPM), cloud workload protection (CWP), application security posture management (ASPM), data security posture management (DSPM), and infrastructure as code (IaC) security — and how they work together

1.2 Describe the purpose and use requirements of one-click sensor deployment

1.3 Describe the purpose and use requirements of the Kubernetes admission controller

2. Cloud Account Registration

2.1 Given a specific use case, determine the most efficient and secure registration method to use for your cloud environment

2.2 Determine which roles are required to perform actions with CrowdStrike Falcon® Cloud Security

2.3 Organize cloud resources into cloud groups to reduce noise and assign responsibility

2.4 Configure cloud security scan exclusion settings

2.5 Troubleshoot issues related to cloud account registrations

3. Cloud Security Policies and Rules

3.1 Given a use case, configure CSPM policies

3.2 Given a use case, recommend an image assessment policy and exclusions

3.3 Given a use case, recommend a Kubernetes admission controller policy configuration

3.4 Given a use case, recommend a runtime sensor policy configuration

4. Pre-Runtime Protection

4.1 Add, edit and delete registry connection details and settings

4.2 Given a use case, recommend an appropriate image assessment method for your environment

4.3 Identify potential security issues — such as malware presence, high-severity Common Vulnerabilities and Exposures (CVEs), detected leaked secrets and Docker file misconfigurations — from the image assessment report

4.4 Identify vulnerabilities and installed packages

5. Runtime Protection

5.1 Determine the best CrowdStrike Falcon® sensor to use when given a specific Kubernetes and container environment configuration

5.2 Troubleshoot issues related to Kubernetes and container sensor deployment

5.3 Identify deployment misconfigurations

5.4 Identify unassessed images used in production

5.5 Identify indicators of attack (IOAs), rogue containers and drift

5.6 Identify network connections

6. Findings and Detection Analysis

6.1 Evaluate cloud security controls and configurations to identify indicators of misconfiguration (IOMs), vulnerabilities and/or high-risk practices

6.2 Identify suspicious/malicious activity (IOAs) and associated persistence mechanisms

6.3 Audit user account activity and permissions to identify risks

6.4 Compare cloud, Docker and Kubernetes configurations to the latest industry benchmarks to determine compliance

6.5 Find unmanaged, public-facing cloud and container assets

7. Remediating and Reporting Issues

7.1 Identify recommended remediation steps for findings and detections

7.2 Describe the purpose and use requirements of scheduled reports for cloud security

7.3 Describe the purpose and use requirements of CrowdStrike Falcon® Fusion SOAR workflows to notify individuals about cloud-related policies, detections, incidents, infrastructure as code and image assessments

CROWDSTRIKE
UNIVERSITY