CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCSE Certification Exam Guide

Description

Successful completion of the CrowdStrike Certified SIEM Engineer (CCSE) exam is required to earn the CCSE certification. This exam evaluates a candidate's knowledge, skills, and abilities to implement and manage CrowdStrike Falcon® Next-Gen SIEM to support security operations.

A successful CrowdStrike Certified SIEM Engineer:

- Understands the key features of Falcon Next-Gen SIEM and role-based access permissions and can enable them to configure, navigate, and manage security information and event management (SIEM) workflows effectively
- Onboards and integrates third-party data sources using data connectors, the Falcon Log Collector, and other supported ingestion methods
- Has experience in parsing and log management — including data collection, normalization, retention, and disposal — and can monitor and troubleshoot log ingestion issues
- Writes basic queries using CrowdStrike Query Language (CQL) to retrieve, analyze, and filter security data efficiently
- Can interpret SIEM alerts, work collaboratively within the Incident Workbench, and use and understand the correlation rules feature
- Has foundational knowledge of CrowdStrike Falcon® Fusion SOAR, enabling them to use prebuilt workflows for automated incident response
- Has at least six (6) months of experience working in the CrowdStrike Falcon® platform

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 the Falcon platform in a production environment.
- Candidates should be able to read English with sufficient accuracy and fluency to support comprehension. Exams are suitable for non-native English speakers.

About the Exam

Assessment Method

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

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCSE certification exam
- Refrain from conduct that violates the CrowdStrike Certification Exam Agreement

In the event of suspected misconduct by the candidate, CrowdStrike reserves the right to invalidate an exam score and take additional action as outlined in the 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 CCSE 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 SIEM Engineer courses in CrowdStrike University to prepare for the CCSE exam. To learn more about these courses, view the CrowdStrike University Training Catalog.

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. User Management
2. Data Ingestion
3. Parsing
4. Content Creation
5. Automation and Integration

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, outlines, 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. User Management

1.1 Configure required user roles and permissions

1.2 Create custom roles

2. Data Ingestion

2.1 Identify first-party and third-party data

2.2 Differentiate appropriate ingest methods for data integration

2.3 Configure and manage built-in data connectors

2.4 Define common components of third-party data source connectors

2.5 Identify necessary sizing requirements for log collector clients

2.6 Configure and deploy the Falcon Log Collector

2.7 Configure fleet management

2.8 Monitor and troubleshoot ingestion issues

3. Parsing

3.1 Understand the CrowdStrike Parsing Standards

3.2 Apply the CrowdStrike Parsing Standard for data normalization

3.3 Identify log formats

3.4 Create parser test cases

3.5 Clone and modify default parsers

3.6 Create custom parsers

3.7 Create an AI-generated parser

3.8 Apply advanced language features for parsing

3.9 Monitor and troubleshoot parsing errors

4. Content Creation

4.1 Manage, create, and utilize lookup files

4.2 Utilize built-in dashboards to monitor activity

4.3 Design and build CQL queries

4.4 Optimize CQL queries

4.5 Create custom dashboards

4.6 Create correlation rules

4.7 Manage and tune correlation rules

4.8 Distinguish between first-party and third-party detections

5. Automation and Integration

5.1 Leverage Falcon Fusion SOAR workflows for automation

5.2 Create API access tokens

5.3 Leverage APIs through FalconPy

CROWDSTRIKE
UNIVERSITY