CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCSA Certification Exam Guide

Description

Successful completion of the CrowdStrike Certified SIEM Analyst (CCSA) exam is required to earn the CCSA certification. This exam evaluates a candidate's knowledge, skills, and abilities with the application of analytical reasoning and investigation skills within the CrowdStrike Falcon® Next-Gen SIEM environment.

A successful CrowdStrike Certified SIEM Analyst:

- Can investigate detections and analyze data using CrowdStrike Query Language (CQL)
- Visualizes and summarizes data and correlates events across multiple data sources to assess and accurately identify suspicious or malicious activity
- Uses first-party and third-party data available in Falcon Next-Gen SIEM to detect threats, interpret alert context, and contribute to incident investigations without needing detailed procedural guidance
- Possesses a foundational understanding of the MITRE ATT&CK® framework and can differentiate between detection types (e.g., first-party, third-party passthrough, and correlation rules)
- Uses Falcon Next-Gen SIEM dashboards for analysis and case management to aggregate incident-related detections, findings, and notes
- Uses data and outputs to create visualizations and reports to communicate event details to leadership
- Has at least six (6) months of experience working in the CrowdStrike Falcon® platform and also has hands-on experience in a security operations center (SOC), threat detection, or incident response role

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 candidates can view and print their CrowdStrike certification exam score report through Pearson.

Recommended Certification Candidate Competence and Abilities

- At least six (6) months of experience with CrowdStrike Falcon in a production environment
- Hands-on experience in a SOC, threat detection, or incident response role
- Sufficient English reading ability to support comprehension (exams are suitable for non-native English speakers)

About the Exam

Assessment Method

The CCSA exam is a 90-minute, 60-question assessment. All exam questions are multiple-choice.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCSA certification exam
- Refrain from any 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 CCSA 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 Analyst courses in CrowdStrike University to prepare for the CCSA exam. To learn more about these courses, view the CrowdStrike 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. Querying and Analytics
2. Detection Logic and Alert Analytics
3. Incident Investigation
4. Reporting and Communication

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. Querying and Analytics

1.1 Construct CQL searches using filters, logical operators, and time parameters

1.2 Leverage dashboards and prebuilt scripts to hunt and analyze for suspicious behaviors

1.3 Interpret query results to identify suspicious or malicious behaviors

1.4 Apply analytical reasoning to pivot and correlate between related Falcon Next-Gen SIEM data sets (network, host, email, etc.)

1.5 Utilize the CrowdStrike Parsing Standard to perform data source agnostic queries

2. Detection Logic and Alert Analysis

2.1 Explain the purpose and function of correlation rules within Falcon Next-Gen SIEM

2.2 Differentiate between detection types in Falcon Next-Gen SIEM (first-party detections, third-party passthrough detections, and correlation rule detections)

2.3 Apply the components of the MITRE ATT&CK framework used in Falcon Next-Gen SIEM

2.4 Differentiate false positives from legitimate detections based on event context

2.5 Understand alert metadata (severity, tactic, confidence) and investigative priority

3. Incident Investigation

3.1 Construct the chain of events for a detection by correlating logs from multiple data sources

3.2 Identify lateral movement, persistence, and privilege escalation indicators

3.3 Pivot between related observables (IP, user, or other indicators)

3.4 Assess incident severity and scope based on correlated evidence

3.5 Recommend response action and/or remediation steps based on findings

3.6 Utilize existing Falcon Fusion SOAR workflows to contain or remediate malicious activity

3.7 Identify and interpret indicators of compromise (IOCs)

3.8 Leverage contextual data (geolocation, IP reputation, or TTPs) to assess threat relevance

3.9 Identify available data sources and retention

4. Reporting and Communication

4.1 Document and summarize investigation results using Case Management

4.2 Use aggregations and visual summaries to reveal trends and anomalies

CROWDSTRIKE UNIVERSITY