CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFR Certification Exam Guide

Description

The CrowdStrike Certified Falcon Responder (CCFR) exam is the final step toward the completion of CCFR certification. This exam evaluates a candidate's knowledge, skills and abilities to respond to a detection within the CrowdStrike Falcon® console.

A successful CrowdStrike Certified Falcon Responder:

- A successful CrowdStrike Certified Falcon Responder:
- Responds to cyber incidents detected within an enterprise network environment using the Falcon console
- Manages filtering, grouping, assignment, commenting and status changes of detections
- Performs basic investigation tasks such as host search, host timeline, process timeline, user search and other workflows
- Conducts basic proactive hunting across enterprise event data and escalates for further analysis and resolution when necessary
- Has at least six (6) months of experience working in the 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 VUE.

University Subscription

It is **strongly suggested** that all exam registrants have an active subscription to CrowdStrike University and have confirmed access to their CrowdStrike University account.

- CrowdStrike certification-aligned courses are available to learners with an active CrowdStrike University account.
- A unique CrowdStrike Certification 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 VUE.

Required 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 CCFR exam is a 90-minute, 60-question assessment.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCFR 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 VUE.

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 CCFR 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 CSU LP- R: Incident Responder courses in CrowdStrike University to prepare for the CCFR 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 CCFR exam:

- Falcon Management — Falcon Console User Guide, Dashboards and Reports section
- Endpoint Security — Start Up and Scale Up, Monitoring, Event Investigation and Response sections

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.

- 1.0 MITRE ATT&CK® Framework Application
- 2.0 Detection Analysis
- 3.0 Event Search
- 4.0 Event Investigation
- 5.0 Search Tools
- 6.0 Falcon Real Time Response (RTR)

Scope Changes

To better reflect the content of the exam and for clarity purposes, the guidelines below 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:

1.0 ATT&CK Framework Application

- 1.1 Understand what information the MITRE ATT&CK framework provides
- 1.2 Apply MITRE ATT&CK tactics and techniques within Falcon to provide context to a detection

2.0 Detection Analysis

- 2.1 Recommend courses of action based on the analysis of information provided within Falcon
- 2.2 Interpret information displayed in the Endpoint security > Activity dashboard
- 2.3 Interpret information displayed in Endpoint security > Endpoint detections
- 2.4 Determine appropriate response to an activity based on detection source
- 2.5 Understand use cases for built-in OSINT tools
- 2.6 Explain what contextual event data is available in a detection (IP/DNS/Disk/etc.)
- 2.7 Triage a detection using filtering, grouping, and sort-by
- 2.8 Evaluate the impact of internal and external prevalance
- 2.9 Evaluate an activity and determine a response based on information displayed in the Full Detection view
- 2.10 Interpret the data provided in the View As Process Tree, View As Process Table and View As Process Activity
- 2.11 Identify managed/unmanaged Neighbors for an endpoint during a Host Search
- 2.12 Understand an IOC and the different types of actions available via Falcon
- 2.13 Distinguish the uses cases for various Hash Management Actions (Block, Block and Hide Detection, Detect Only, Allow, No action)
- 2.14 Understand the effects of allowlisting and blocklisting
- 2.15 Explain the effects of machine learning exclusion rules, sensor visibility exclusions, and IOA exclusions
- 2.16 Apply best practices to quarantined files

3.0 Event Search

- 3.1 Perform an Event Advanced Search from a detection and refine a search using event actions
- 3.2 Determine when and why to use specific event actions
- 3.3 Distinguish between commonly used event types

4.0 Event Investigation

- 4.1 Explain what information a Process Timeline will provide
- 4.2 Explain what information a Hosts Timeline will provide
- 4.3 Understand when to pivot to a Process Timeline or Process Explorer from an Event Search
- 4.4 Analyze process relationships (parent/child/sibling) using the information contained in the Full Detection Details

5.0 Search Tools

- 5.1 Analyze the information provided in a User Search
- 5.2 Analyze the information provided in an IP Search
- 5.3 Analyze the information provided in a Hash Search
- 5.4 Interpret the data contained in Host Search results
- 5.5 Analyze the information provided in a Bulk Domain Search

6.0 Real Time Response (RTR)

- 6.1 Explain the technical capabilities of Real Time Response
- 6.2 Identify administrative requirements for Real Time Response settings
- 6.3 Determine when and how to connect to a host
- 6.4 Investigate a threat within Falcon and use RTR commands to remediate it
- 6.5 Utilize custom scripts in RTR to remediate a threat
- 6.6 Set up a Workflow with RTR custom scripts
- 6.7 Review audit logs to audit Real time response activity

CROWDSTRIKE UNIVERSITY