CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFH Certification Exam Guide

Description

The CrowdStrike Certified Falcon Hunter (CCFH) exam is the final step toward the completion of the CCFH 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 Falcon Hunter:

- Understands all aspects of detection investigation
- Navigates among and uses multiple views in the Falcon console to perform automated queries such as IP and domain searches and time-lining using CQL event searching
- Understands event data structure and relationships
- Conducts simple and intermediate search queries using CQL

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 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.

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 CCFH exam is a 90-minute, 60-question assessment.

Initial Certification

To be eligible for certification, candidates must:

- Achieve a passing score on the CCFH 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 CCFH 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 Falcon Hunter courses in CrowdStrike University AND attain six months practical experience to prepare for the CCFH 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 CCFH exam:

- Falcon Management
- Endpoint Security
- Monitoring
- Event Investigation

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. MITRE ATT&CK® Frameworks
2. Detection Analysis
3. Search and Investigation Tools
4. Event Search
5. Reports and References
6. Hunting Analytics
7. Hunting Methodology

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. ATT&CK Frameworks

1.1 Demonstrate knowledge of the cyber kill chain (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, covering tracks) and recognize intelligence gaps

1.2 Utilize the MITRE ATT&CK Framework to model threat actor behaviors

1.3 Operationalize the MITRE ATT&CK Framework to look for research threat models, TTPs and threat actors, and pivot as necessary and convey to non-technical audiences

2. Detection Analysis

2.1 Analyze information displayed in the Host Timeline to understand host states and events

2.2 Analyze the information displayed in the Process Timeline to understand the flow of events and detections

2.3 Pivot from the detection page to additional investigative tools

3. Search and Investigation Tools

3.1 Analyze and interpret metadata around files and processes recorded by Falcon

3.2 Differentiate use of Investigate Module tools available in Falcon

3.3 Understand use cases for various search options (e.g., User Search, Host Search, Hash Search, IP Addresses Search, Bulk Domain Search)

3.4 Interpret search result information displayed in dashboards to determine additional investigation or action

4. Event Search

4.1 Define key syntax of CrowdStrike Query Language (CQL)

4.2 Build a query and perform a search using CQL

4.3 Format event data for user readability, export or charting

4.4 Filter event data and analyze results

4.5 Describe the process relationship of (Target/Parent/Context)

4.6 Define key data event types

4.7 Convert and format Unix times to UTC readable time

4.8 Create a custom dashboard to display Advanced Event Search results

5. Reports and References

5.1 Use the built-in Hunt reports to refine event details

5.2 Use the built-in Visibility reports to refine event details

5.3 Leverage the Events Full Reference documentation to learn information about specific events

6. Hunting Analytics

6.1 Analyze and recognize suspicious overt malicious behaviors

6.2 Understand target systems (asset inventory and who would target those assets)

6.3 Evaluate information for reliability, validity and relevance for use in the process of elimination

6.4 Identify alternative analytical interpretations to minimize and reduce false positives

6.5 Decode and understand PowerShell/CMD activity

6.6 Recognize patterns such as an enterprise-wide file infection process to determine the root cause or source of the infection

6.7 Differentiate testing, DevOPs or general user activity from adversary behavior

6.8 Identify the vulnerability exploited from an initial attack vector

7. Hunting Methodology

7.1 Conduct routine active hunt operations within your environment in order to determine if your environment has been breached

7.2 Perform outlier analysis with the Falcon tool

7.3 Conduct hypothesis and hunting lead generation in order to prove them using Falcon tools

7.4 Construct simple and complex EAM queries in Falcon

7.5 Investigate a process tree