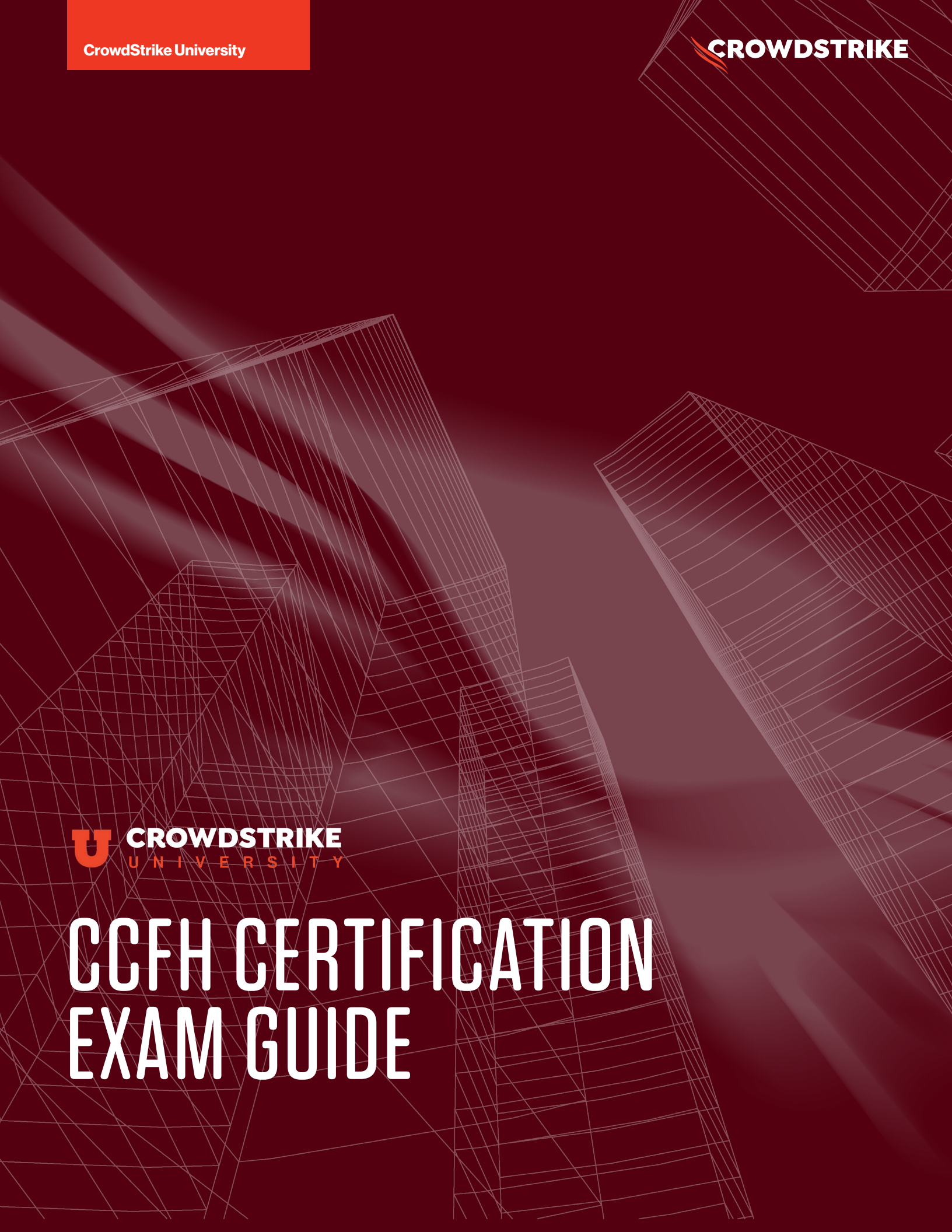
CrowdStrike University

CROWDSTRIKE



CROWDSTRIKE UNIVERSITY

CCFH CERTIFICATION EXAM GUIDE

DESCRIPTION

The CrowdStrike Certified Falcon Hunter (CCFH) exam is the final step toward the completion of CCFH certification. This exam evaluates a candidate's knowledge, skills and abilities to effectively respond to a detection within the CrowdStrike Falcon® console and Investigate app, use queries and automated reports to assist in machine auditing and proactive investigation, and perform search queries using the Splunk syntax.

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 Splunk event searching
- Understands event data structure and relationships
- Conducts simple and intermediate search queries using Splunk Search Processing Language (SPL)

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

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 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 CCFH exam is a 90-minute, 60-question assessment. This exam passed several rounds of editing by both technical and non-technical experts and has been tested by a wide variety of candidates.

INITIAL CERTIFICATION

To be eligible for certification, candidates must:

- Achieve 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 at Pearson VUE.

RETAKE POLICY

Candidates who do not pass an exam on their first (1st) attempt:

- Must wait 24 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 (2nd) attempt, a candidate will need to wait seven (7) days for the third (3rd) attempt and any subsequent attempts. Wait time begins the day after the attempt.

Candidates who want to retake the exam should consider re-sitting the applicable recommended course(s) and gain additional experience with CrowdStrike Falcon before trying again.

Retakes beyond the fourth (4th) 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 for a fifth (5th) 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 CS Certification Manager before clearing him or her 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

Certification exams are not tied to product versions. The following lifecycle will apply to recertification moving forward, beginning with the date the certification was issued:

- CrowdStrike Certified Falcon Administrator (CCFA): 3 years
- CrowdStrike Certified Falcon Responder (CCFR): 3 years
- CrowdStrike Certified Falcon Hunter (CCFH): 3 years

EXAM PREPARATION

RECOMMENDED TRAINING

CrowdStrike strongly recommends that certification candidates complete these **CSU LP-H: Threat 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**. CrowdStrike also recommends that candidates physically access the Falcon console and perform the exam objectives as a form of practice.

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 competency areas 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 Attack Frameworks
2.0 Detection Analysis
3.0 Search Tools
4.0 Event Search
5.0 Reports
6.0 Hunting Analytics
7.0 Hunting Methodology
8.0 Documentation

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 ATTACK FRAMEWORKS

- 1.1 Demonstrate knowledge of the cyber kill chain (7) stages (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 Explain when to use Event Search
- 2.2 Explain what a Process Timeline will provide
- 2.3 Demonstrate how to get a Process Timeline
- 2.4 Explain what a Host Timeline will provide

3 SEARCH TOOLS

- 3.1 Explain how to extract, analyze and use metadata around files and processes related to the Falcon platform
- 3.2 Explain what information a bulk (Destination) IP search provides
- 3.3 Pivot on results (PID vs. Process ID, etc.)
- 3.4 Explain what information a User Search provides
- 3.5 Explain what information a Host Search provides
- 3.6 Explain what information a Source IP Search provides
- 3.7 Explain what information a Hash Search provides
- 3.8 Explain what information a Hash Execution Search provides
- 3.9 Explain what information a Bulk Domain Search provides
- 3.10 Write an effective custom alert rule
- 3.11 Explain what event actions do

4 EVENT SEARCH

- 4.1 Describe general use cases for event searching
- 4.2 Perform a basic keyword search
- 4.3 Use Splunk syntax to refine your search (using fields such as ComputerName, event_simpleName, etc.)
- 4.4 Use interesting fields to refine your search
- 4.5 From the Statistics tab, use the left click filters to refine your search
- 4.6 Describe the process relationship of (Target/Parent/Context)
- 4.7 Explain how the rename command is used in a query related to associated event data, such as parent/target/context relationships
- 4.8 Explain what the “table” command does and demonstrate how it can be used for formatting output
- 4.9 Explain what the “stats count by” command does and demonstrate how it can be used for statistical analysis
- 4.10 Explain what the “join” command does and how it can be used to join disparate queries
- 4.11 Explain key event data types
- 4.12 Export search results
- 4.13 Convert and format Unix times to UTC-readable time

5 REPORTS

- 5.1 Explain what information a Linux Sensor Report will provide
- 5.2 Explain what information a Mac Sensor Report will provide
- 5.3 Locate built-in Hunting reports and explain what they provide
- 5.4 Explain what information the PowerShell Hunt report provides and demonstrate how to filter it
- 5. 5 Demonstrate the ability to find built-in visibility reports and explain what they provide

6 HUNTING ANALYTICS

- 6.1 Analyze and recognize suspicious overt malicious behaviors
- 6.2 Demonstrate knowledge of 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 and attempting 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 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 to prove them out using Falcon tools
- 7.4 Construct simple and complex EAM queries in Falcon
- 7.5 Investigate a process tree

8 DOCUMENTATION

- 8.1 Explain what information is in the Events Data Dictionary (Event Index)
- 8.2 Explain what information is in the Hunting & Investigation Guide