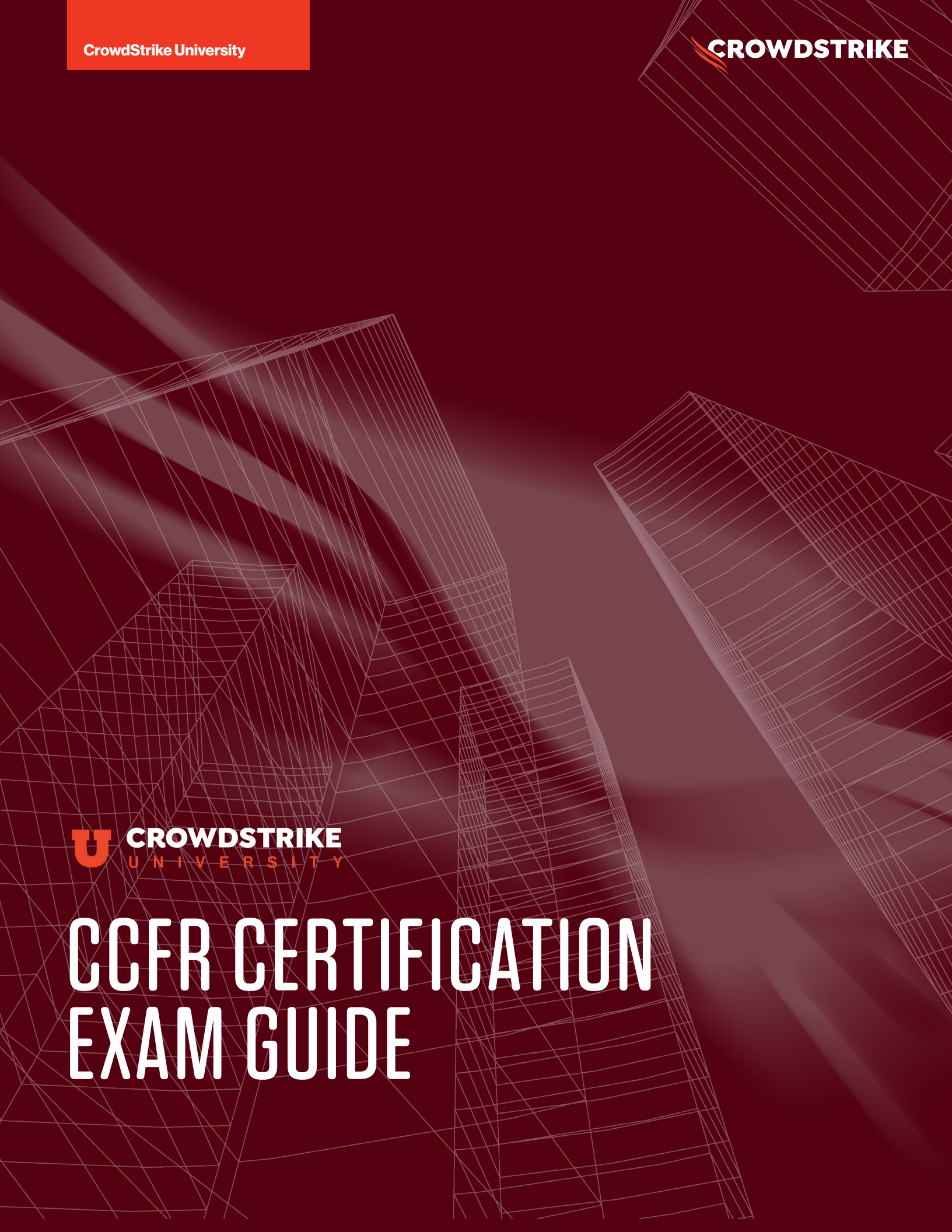
CrowdStrike University

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:

- Conducts initial triage of detections in 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 click-driven workflows
- Conducts basic proactive hunting for atomic indicators such as domain names, IP addresses and hash values across enterprise event data

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 CCFR exam is a 90-minute, 60-question assessment. Exam questions have been specifically written in a way that eliminates tricky wording, double negatives, and/or fill-in-the-blank type questions. 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 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 at Pearson VUE.

RETAKE POLICY

Candidates who do not pass an exam on their first (1st) 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 (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 that want to retake the exam should consider re-sitting the applicable recommended course(s) and gain additional experience with the CrowdStrike Falcon platform 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 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

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 certification candidates complete these **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 Attack Frameworks
- 2.0 Detection Analysis
- 3.0 Event Search
- 4.0 Hunting Analytics

- 5.0 Hunting Methodology
- 6.0 Navigation
- 7.0 Reports
- 8.0 Search Tools

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 ATTACK FRAMEWORKS

- 1.1 Use MITRE ATT&CK information within Falcon to provide context to a detection
- 1.2 Explain what information the MITRE ATT&CK framework provides

2.0 DETECTION ANALYSIS

- 2.1 Recommend courses of action based on the analysis of information provided within the Falcon platform
- 2.2 Explain what general information is on the Detections dashboard
- 2.3 Explain what information is in the Activity > Detections page
- 2.4 Describe the different sources of detections within the Falcon platform
- 2.5 Interpret the data contained in Host Search results
- 2.6 Interpret the data contained in Hash Search results
- 2.7 Demonstrate how to pivot from a detection to a Process Timeline
- 2.8 Explain what contextual event data is available in a detection (IP/DNS/Disk/etc.)

- 2.9 Explain how detection filtering and grouping might be used
- 2.10 Explain when to use built-in OSINT tools
- 2.11 Explain the difference between Global vs. Local Prevalence
- 2.12 Explain what Full Detection Details will provide
- 2.13 Explain how to get to Full Detection Details
- 2.14 Analyze process relationships using the information contained in the Full Detection Details
- 2.15 Explain what type of data the View As Process Tree, View As Process Table and View As Process Activity provide
- 2.16 Explain how to identify managed/unmanaged Neighbors for an endpoint during a Host Search
- 2.17 Explain the purpose of assigning a detection to an analyst
- 2.18 Triage a non-Falcon Indicator of Compromise (IOC) in the Falcon UI
- 2.19 Describe what the different policies (Block, Block and Hide Detection, Detect Only, Allow, No Action) do
- 2.20 Explain the effects of allowlisting and blocklisting
- 2.21 Explain the effects of machine learning exclusion rules
- 2.22 Explain the effects of Sensor Visibility exclusions
- 2.23 Explain the effects of IOA exclusions
- 2.24 State the retention period for quarantined files
- 2.25 Describe what happens when you release a quarantined file
- 2.26 Download a quarantined file
- 2.27 Based on a detection, determine which investigate tools, e.g., host, hash, etc., to use based on best practices

3.0 EVENT SEARCH

- 3.1 Perform an Event Search from a detection and refine a search using event actions
- 3.2 Explain what event actions do
- 3.3 Explain key event types

4.0 HUNTING ANALYTICS

- 4.1 Explain what information a process Timeline will provide
- 4.2 Explain what information a Host Timeline will provide

5.0 HUNTING METHODOLOGY

- 5.1 Describe the process relationship (Target/Parent/Context)

6.0 NAVIGATION

- 6.1 Retrieve the information required to generate a Process Timeline
- 6.2 Demonstrate how to get to a Process Explorer from a Event Search
- 6.3 Find quarantined files

7.0 REPORTS

- 7.1 Export detection and process data from Full Detection Details for further review
- 7.2 Explain what information is in the Detection Activity Report
- 7.3 Describe what information is in the Executive Summary Dashboard
- 7.4 Describe what information is in the Detection Resolution Dashboard

8.0 SEARCH TOOLS

- 8.1 Explain what information a User Search provides
- 8.2 Explain what information a IP Search provides
- 8.3 Explain what information a Hash Executions (Search) provides
- 8.4 Explain what information a Hash Search provides
- 8.5 Explain what information a Bulk Domain Search provides