CrowdStrike CCFR-201b Study Guide

GRAB THE CROWDSTRIKE FALCON RESPONDER CERTIFICATION PDF QUESTIONS & ANSWERS

Exam Summary – Syllabus –Questions

CCFR-201B

CrowdStrike Certified Falcon Responder (CCFR)

60 Questions Exam – 80% Cut Score – Duration of 90 minutes

www.VMExam.com

Table of Contents

Get an Overview of the CCFR-201b Certification:

Who should take the CCFR-201b exam? This is the first question that comes to a candidate's mind when preparing for the Falcon Responder certification. The CCFR-201b certification is suitable for candidates who are keen to earn knowledge on the Falcon Platform and grab their CrowdStrike Certified Falcon Responder (CCFR). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But CCFR-201b study guide PDF is here to solve the problem. CCFR-201b PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the CrowdStrike CCFR-201b Certification?

There are several reasons why one should grab the CCFR-201b certification.

- The Falcon Responder certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the CrowdStrike Certified Falcon Responder (CCFR) is a powerful qualification for a prosperous career.

What Is the CrowdStrike CCFR-201b Falcon Responder Certification Exam Structure?

Exam Name	CrowdStrike Falcon Responder
Exam Code	CCFR
Exam Price	$250 USD
Duration	90 minutes
Number of Questions	60
Passing Score	80%
Recommended Training / Books	CCFR Training

Schedule Exam	**PEARSON VUE**
Sample Questions	**CrowdStrike CCFR Sample Questions**
Recommended Practice	**CrowdStrike Certified Falcon Responder (CCFR) Practice Test**

Enhance Knowledge with CCFR-201b Sample Questions:

Question: 1

When reviewing an internal IP address via IP Search, which fields would help determine potential lateral movement?

(Choose two)

a) Host group name
b) MAC address
c) Connected hosts
d) List of destination IPs

Answer: c, d

Question: 2

Advanced Event Search in Falcon supports a look-back period of up to ___________ days depending on the retention policy.

a) 30
b) 1
c) 7
d) 90

Answer: d

Question: 3

When viewing detection information, which component provides granular details like command-line arguments and file paths?

a) Host Search
b) Full Detection View
c) Real Time Response
d) Activity Dashboard

Answer: b

Question: 4

User Search can help correlate suspicious behavior by showing all of the following except:

a) Processes launched by the user
b) Group policies applied to the user
c) Detection events involving the user
d) Hostnames where the user has logged in

Answer: b

Question: 5

Which search type should be used to investigate whether a suspicious executable has affected multiple hosts?

a) Host Search
b) Hash Search
c) User Search
d) Bulk Domain Search

Answer: b

Question: 6

Which two detection filtering options are available in the Endpoint Security > Endpoint Detections page?

(Choose two)

a) Threat actor
b) Tactic
c) Host group
d) Command hash

Answer: b, c

Question: 7

Which Falcon feature allows responders to assign specific actions to detections such as “Allow” or “Block and Hide”?

a) Detection Rules Manager
b) Policy Editor
c) Host Management Actions
d) IOC Management Console

Answer: c

Question: 8

What would be a logical next step after identifying an unmanaged host in Host Search?

a) Quarantine the host
b) Block its public IP
c) Add the host to a monitoring policy
d) Investigate how it connected and initiate containment

Answer: d

Question: 9

You're investigating suspicious behavior linked to a user. Which key indicators should you examine in the User Search view to assess the threat context?

(Choose two)

a) Number of failed login attempts
b) User's IP subnet
c) Number of hosts the user has accessed
d) Number of detections associated with the user

Answer: c, d

Question: 10

What is the default port used by Falcon RTR to establish a connection with a managed host?

a) 22
b) 443
c) 8443
d) 80

Answer: b

What Study Guide Works Best in Acing the CrowdStrike CCFR-201b Falcon Responder Certification?

The CCFR-201b study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Falcon Responder exam, getting in full touch of the syllabus is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don’t like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the CrowdStrike CCFR-201b training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the CrowdStrike CCFR-201b Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, CCFR-201b practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven CCFR-201b Practice Test for Success!!!

Do you want to pass the CCFR-201b exam on your first attempt? Stop worrying; we, VMExam.com are here to provide you the best experience during your CrowdStrike Falcon Responder preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **CCFR-201b practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.