CrowdStrike CCFH-202b Study Guide

GRAB THE CROWDSTRIKE FALCON HUNTER CERTIFICATION PDF QUESTIONS & ANSWERS

Exam Summary – Syllabus –Questions

CCFH-202B

CrowdStrike Certified Falcon Hunter (CCFH)
60 Questions Exam – 80% Cut Score – Duration of 90 minutes

www.VMExam.com

Table of Contents

Get an Overview of the CCFH-202b Certification:

Who should take the **CCFH-202b exam**? This is the first question that comes to a candidate's mind when preparing for the Falcon Hunter certification. The CCFH-202b certification is suitable for candidates who are keen to earn knowledge on the Falcon Platform and grab their CrowdStrike Certified Falcon Hunter (CCFH). When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But CCFH-202b study guide PDF is here to solve the problem. CCFH-202b PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the CrowdStrike CCFH-202b Certification?

There are several reasons why one should grab the CCFH-202b certification.

- The Falcon Hunter 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 Hunter (CCFH)** is a powerful qualification for a prosperous career.

What Is the CrowdStrike CCFH-202b Falcon Hunter Certification Exam Structure?

Exam Name	CrowdStrike Falcon Hunter
Exam Code	CCFH-202b
Exam Price	$250 USD
Duration	90 minutes
Number of Questions	60
Passing Score	80%
Recommended Training / Books	CCFH Training

Schedule Exam	PEARSON VUE
Sample Questions	CrowdStrike CCFH-202b Sample Questions
Recommended Practice	CrowdStrike Certified Falcon Hunter (CCFH) Practice Test

Enhance Knowledge with CCFH-202b Sample Questions:

Question: 1

Which methods are valid to convert Unix timestamps to human-readable time in Falcon?

(Choose two)

a) Apply custom visualization template
b) Enable auto-conversion in dashboard
c) Manually divide Unix time by 1000
d) Use FORMAT_TIMESTAMP()

Answer: b, d

Question: 2

Which scenarios justify initiating a hypothesis-driven hunt?

(Choose two)

a) Following an alert for abnormal outbound traffic to a rare domain
b) After a vendor releases a critical vulnerability with known exploits
c) To investigate hosts flagged with expired endpoint licenses
d) To verify administrative user compliance with login policy

Answer: a, b

Question: 3

What actions can be taken after filtering event data in the Falcon platform?

(Choose two)

a) Build detection rules
b) Export results to CSV
c) Visualize with dashboards
d) Apply memory patching

Answer: b, c

Question: 4

What behaviors commonly indicate suspicious command prompt (cmd.exe) usage?

(Choose two)

a) Chained commands using logical operators (e.g., &&, |)
b) Execution from system32 folder under admin user
c) CMD launched with a direct connection to PowerShell
d) CMD invoked by explorer.exe during login

Answer: a, c

Question: 5

Which actions can be initiated directly from the detection page in Falcon to pivot into deeper investigation?

(Choose two)

a) View process details
b) Disable user account
c) Run full antivirus scan
d) Initiate Host Timeline view

Answer: a, d

Question: 6

Pivoting from a detection into the _____ Timeline is helpful to identify artifacts created before and after the alert was triggered.

a) Sensor
b) Audit
c) Host
d) Forensic

Answer: c

Question: 7

When multiple domains are under investigation, analysts can utilize the _____ feature in Falcon to streamline analysis.

a) Threat Intelligence Panel
b) Domain Lookup Wizard
c) Domain Behavior Tracker
d) Bulk Domain Search

Answer: d

Question: 8

What is the purpose of constructing complex EAM queries in the hunting process?

a) To suppress known benign alerts
b) To extract actionable insights from large volumes of endpoint telemetry/
c) To create automated remediation workflows
d) To update sensor drivers on legacy systems

Answer: b

Question: 9

A key step in minimizing false positives is understanding the _____ in which a process executes, including user, host role, and time of execution.

a) privilege
b) signature
c) context
d) syntax

Answer: c

Question: 10

Why is the Events Full Reference documentation essential when reviewing unusual activity logs?

a) It allows direct editing of detection rules
b) It defines event types, fields, and expected values
c) It lists CrowdStrike partner threat feeds
d) It contains historical IOC archives

Answer: b

What Study Guide Works Best in Acing the CrowdStrike CCFH-202b Falcon Hunter Certification?

The CCFH-202b 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 Hunter 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 CCFH-202b 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 CCFH-202b 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, CCFH-202b practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven CCFH-202b Practice Test for Success!!!

Do you want to pass the CCFH-202b exam on your first attempt? Stop worrying; we, VMExam.com are here to provide you the best experience during your CrowdStrike Falcon Hunter preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **CCFH-202b practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.