CrowdStrike CCFR

CROWDSTRIKE FALCON RESPONDER CERTIFICATION QUESTIONS & ANSWERS

Exam Summary – Syllabus – Questions

CCFR

CrowdStrike Certified Falcon Responder (CCFR)

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

www.VMExam.com

Table of Contents

Know Your CCFR Certification Well:

The CCFR is best suitable for candidates who want to gain knowledge in the CrowdStrike Falcon Platform. Before you start your CCFR preparation you may struggle to get all the crucial Falcon Responder materials like CCFR syllabus, sample questions, study guide.

But don't worry the CCFR PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CCFR syllabus?
- How many questions are there in the CCFR exam?
- Which Practice test would help me to pass the CCFR exam at the first attempt?

Passing the CCFR exam makes you CrowdStrike Certified Falcon Responder (CCFR). Having the Falcon Responder certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CrowdStrike CCFR Falcon Responder Certification Details:

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**

CCFR Syllabus:

Section	Objectives
ATT&CK Frameworks	- Understand what information the MITRE ATT&CK framework provides - Apply MITRE ATT&CK tactics and techniques within Falcon to provide context to a detection
Detection Analysis	- Recommend courses of action based on the analysis of information provided with Falcon - Interpret information displayed in the Endpoint security > Activity dashboard - Interpret information displayed in Endpoint security > Endpoint detections - Determine appropriate response to an activity based on detection source - Understand use cases for built-in OSINT tools - Explain what contextual event data is available in detection (IP/DNS/Disk/etc.) - Triage a detection using filtering, grouping and sort-by - Evaluate the impact of internal and external prevalance - Evaluate an activity and determine a response based on information displayed in the FullDetection view - Interpret the data provided in the View As Process Tree, View As Process Table and View As Process Activity - Indentify managed/unmanaged Neighbors for an endpoint during a Host Search - Understand an IOC and the different types of actions available via Falcon - Distinguish the uses cases for various Has Management Actions (Block, Block and Hide Detection, Detect Only, Allow, No action) - Understand the effects of allowlisting and blocklisting - Explain the effects of machine learning exclusion rules, sensor visibility exclusions, and IOA exclusions - Apply best practices to quarantined files
Event Search	- Perform an Event Advanced Search from a detection and refine a search using event actions - Determine when and why to use specific event actions

Section	Objectives
	- Distinguish between commonly used event types
Event Investigation	- Explain what information a Process Timeline will provide - Explain what information a Hosts Timeline will provide - Understand when to pivot to a Process Timeline or Process Explorer from an Event Search - Analyze process relationships (parent/child/sibling) using the information contained in the Full Detection Details
Search Tools	- Analyze the information provided in a User Search - Analyze the information provided in an IP Search - Analyze the information provided in a Hash Search - Analyze the information provided in Host Search results - Analyze the information provided in a Bulk Domain Search
Real Time Response (RTR)	- Explain the technical capabilities of Falcon Real Time Response - Identify administrative requirements for Real Time Response settings - Determine when and how to connect to a host - Investigate a threat within Falcon and use RTR commands to remediate it - Utilize custom scripts in RTR to remediate a threat - Set up a Workflow with RTR custom scripts - Review audit logs to audit RTR activity

CrowdStrike CCFR 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

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: 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

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: 5

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: 6

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: 7

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: 8

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: 9

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: 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

Study Guide to Crack CrowdStrike Falcon Responder CCFR Exam:

- Getting details of the CCFR syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CCFR exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CrowdStrike provided training for CCFR exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CCFR sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CCFR practice tests is must. Continuous practice will make you an expert in all syllabus areas.