Pass CCFH-202b Falcon Hunter Exam: Study Tips & Resources!

CROWDSTRIKE FALCON HUNTER CERTIFICATION QUESTIONS & ANSWERS

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CCFH-202B

CrowdStrike Certified Falcon Hunter (CCFH)

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

Table of Contents

Get Ready for the CCFH-202b Exam:

Prepare effectively for the CCFH-202b exam using reliable **study strategies and methods**. Enhance your preparedness, deepen your understanding of the Falcon Platform, and enhance your likelihood of achieving success in the CrowdStrike CrowdStrike Certified Falcon Hunter (CCFH) with our comprehensive guide. Embark on your path to exam excellence today.

Know More About the CrowdStrike Certified Falcon Hunter (CCFH) Certification:

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**

Learn More About the CCFH-202b Syllabus:

Section	Objectives
ATT&CK Frameworks	- Demonstrate knowledge of the cyber kill chain (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, covering tracks) and recognize intelligence gaps - Utilize the MITRE ATT&CK Framework to model threat actor behaviors

Section	Objectives
	- 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
Detection Analysis	- Analyze information displayed in the Host Timeline to understand host states and events - Analyze the information displayed in the Process Timeline to understand the flow of events and detections - Pivot from the detection page to additional investigative tools
Search and Investigation Tools	- Analyze and interpret metadata around files and processes recorded by Falcon - Differentiate use of Investigate Module tools available in Falcon - Understand use cases for various search options (e.g., User Search, Host Search, Hash Search, IP Addresses Search, Bulk Domain Search) - Interpret search result information displayed in dashboards to determine additional investigation or action
Event Search	- Define key syntax of CrowdStrike Query Language (CQL) - Build a query and perform a search using CQL - Format event data for user readability, export or charting - Filter event data and analyze results - Describe the process relationship of (Target/Parent/Context) - Define key data event types - Convert and format Unix times to UTC readable time - Create a custom dashboard to display Advanced Event Search results
Reports and References	- Use the built-in Hunt reports to refine event details - Use the built-in Visibility reports to refine event details - Leverage the Events Full Reference documentation to learn information about specific events
Hunting Analytics	- Analyze and recognize suspicious overt malicious behaviors

Section	Objectives
	- Understand target systems (asset inventory and who would target those assets) - Evaluate information for reliability, validity and relevance for use in the process of elimination - Identify alternative analytical interpretations to minimize and reduce false positives - Decode and understand PowerShell/CMD activity - Recognize patterns such as an enterprise-wide file infection process to determine the root cause or source of the infection - Differentiate testing, DevOPs or general user activity from adversary behavior - Identify the vulnerability exploited from an initial attack vector
Hunting Methodology	- Conduct routine active hunt operations within your environment in order to determine if your environment has been breached - Perform outlier analysis with the Falcon tool - Conduct hypothesis and hunting lead generation in order to prove them using Falcon tools - Construct simple and complex EAM queries in Falcon - Investigate a process tree

Prepare with CCFH-202b Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 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

Tips for Success in the CrowdStrike Falcon Hunter Exam:

Familiarize Yourself with the CCFH-202b Exam Format:

Before starting your study regimen, it's crucial to acquaint yourself with the structure of the CCFH-202b exam. Take a moment to **review the exam syllabus**, grasp the test format, and pinpoint the main areas of concentration. Having prior knowledge of the exam's layout will assist you in customizing your study strategy effectively.

Create A Study Timetable for the CCFH-202b Exam:

To prepare efficiently for the CCFH-202b exam, devise a study schedule that aligns with your lifestyle and preferred learning approach. Allocate dedicated time slots for studying each day, prioritizing topics according to their significance and your level of proficiency. Maintaining consistency by adhering to your schedule and steering clear of procrastination is imperative.

Diversify Your Study Sources:

Ensure you broaden your study material beyond just one source. Use various resources like textbooks, online courses, practice exams, and study guides to

understand the CCFH-202b exam subjects thoroughly. Each resource provides distinct perspectives and explanations that can enrich your learning journey.

Regular Practice for the CCFH-202b Exam:

Consistent practice is essential for effective preparation for the CCFH-202b exam. Engaging in regular practice enables you to strengthen your grasp of essential concepts, improve your problem-solving abilities, and become accustomed to the exam format. Allocate dedicated time to solving practice questions and sample tests to assess your progress accurately.

Allow for Rest and Breaks:

While studying is crucial, taking breaks and rest is equally vital. Pushing yourself too hard without sufficient rest can result in burnout and reduced effectiveness. Incorporate short breaks into your study sessions to recharge and stay focused.

Maintain Organization Throughout Your CCFH-202b Exam Preparation:

Keep yourself organized as you prepare for the CCFH-202b exam by monitoring your progress and managing your materials effectively. Ensure your study area remains neat, utilize folders or digital aids to arrange your notes and resources, and develop a checklist of topics to review. Employing an organized approach will assist you in staying focused and reducing stress levels.

Seek Guidance from Mentors:

Feel free to ask for clarification when you come across confusing or difficult concepts during your study sessions. Seek support from peers, instructors, or online forums to address any uncertainties. Addressing doubts will prevent misunderstandings and ensure you develop a strong **understanding of the material**.

Regular Review is Crucial for the CCFH-202b Exam:

Frequent revisiting of material is paramount for retaining information over the long term. Revisit topics you've already covered to strengthen your comprehension and pinpoint areas that need further focus. Regular review sessions will **solidify your understanding** and enhance your confidence.

Master Time Management for the CCFH-202b Exam:

Skillful time management is essential on the exam day to ensure you finish all sections within the designated time limits. During your practice sessions, replicate

the conditions of the CCFH-202b exam and practice managing your time accordingly. Formulate strategies for efficiently addressing each section to optimize your score.

Have A Positive Mindset:

Finally, maintain a positive attitude and have faith in your capabilities. Stay confident in your preparation and trust that you are well-prepared to handle the CCFH-202b exam. Envision success, remain focused, and approach the exam calmly and objectively.

Benefits of Passing the CCFH-202b Exam:

- Completing the CCFH-202b exam unlocks pathways to fresh career prospects and progression within your industry.
- The extensive preparation needed for the CCFH-202b certification equips you with comprehensive knowledge and practical expertise applicable to your field.
- Possessing the CCFH-202b certification showcases your mastery and dedication to excellence, garnering acknowledgment from both peers and employers.
- Certified professionals often command higher salaries and have greater potential for earning than those without certification.
- Acquiring the CCFH-202b certification validates your competence and trustworthiness, fostering confidence among clients, employers, and peers.

Explore the Trusted Practice Exam for the CCFH-202b Certification:

At VMExam.com, you'll find comprehensive resources for the CCFH-202b exam. Our platform offers authentic practice exams tailored specifically for the CCFH-202b certification. What advantages do these practice exams provide? You'll encounter genuine exam-style questions expertly crafted by industry professionals, allowing you to improve your performance in the exam. Rely on VMExam.com for rigorous, unlimited access to **CCFH-202b practice exams** for two months, allowing you to boost your confidence steadily. Through focused practice, numerous candidates have successfully streamlined their path to achieving the CrowdStrike Certified Falcon Hunter (CCFH).

Final Remarks:

Preparing for the CCFH-202b examination demands commitment, strategic planning, and efficient study methods. Implementing these study suggestions can enrich your preparation, elevate your self-assurance, and increase your likelihood of excelling in the exam. Keep your focus sharp, maintain organization, and believe in your abilities. Best of luck!