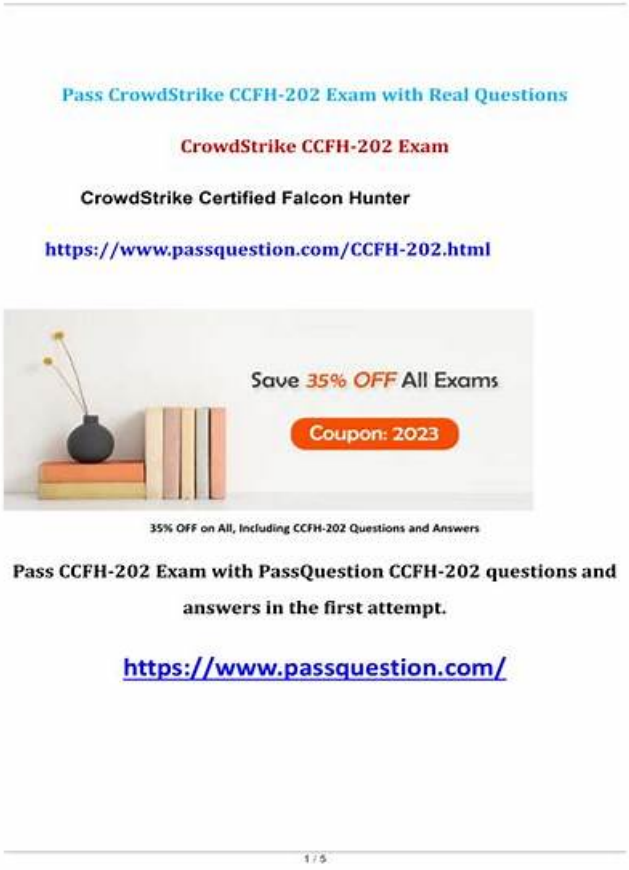
Exam CCFH-202b Syllabus - CCFH-202b Training Questions



You should also keep in mind that to get success in the CrowdStrike CCFH-202b exam is not an easy task. The CrowdStrike CCFH-202b certification exam always gives a tough time to their candidates. So you have to plan well and prepare yourself as per the recommended CCFH-202b Exam study material.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Event Search: This domain focuses on using CrowdStrike Query Language to build queries, format and filter event data, understand process relationships and event types, and create custom dashboards.
Topic 2	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 3	• ATT&CK Frameworks: This domain covers understanding the cyber kill chain and using the MITRE ATT&CK Framework to model threat actor behaviors and communicate findings to non-technical audiences.
Topic 4	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.

>> Exam CCFH-202b Syllabus <<

CCFH-202b Training Questions, CCFH-202b Test Tutorials

Many candidates find the CrowdStrike CCFH-202b exam preparation difficult. They often buy expensive study courses to start their CrowdStrike Certified Falcon Hunter (CCFH-202b) certification exam preparation. However, spending a huge amount on such resources is difficult for many CrowdStrike exam applicants. The latest CrowdStrike CCFH-202b Exam Dumps are the right option for you to prepare for the CCFH-202b certification test at home. ActualTorrent has launched the CCFH-202b exam dumps with the collaboration of world-renowned professionals.

CrowdStrike Certified Falcon Hunter Sample Questions (Q60-Q65):

NEW QUESTION # 60
What is the difference between a Host Search and a Host Timeline?

- A. There is no difference. You just get to them different ways
- B. A Host Search organizes the data in useful event categories like process executions and network connections, a Host Timeline provides an uncategorized view of recorded events in chronological order
- C. You access a Host Search from a detection to show you every recorded process event related to the detection and you can only populate the Host Timeline fields manually
- D. Host Search is used for detection investigation and Host Timeline is used for proactive hunting

Answer: B

Explanation:
This is the difference between a Host Search and a Host Timeline. A Host Search is an Investigate tool that allows you to view events by category, such as process executions, network connections, file writes, etc. A Host Timeline is an Investigate tool that allows you to view all events in chronological order, without any categorization. Both tools can be used for detection investigation and proactive hunting, depending on the use case and preference. You can access a Host Search from a detection or manually enter the host details. You can also populate the Host Timeline fields manually or from other pages in Falcon.

NEW QUESTION # 61
In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

- A. Displays only the command lines containing "badstring"
- B. Highlights "badstring" in all command lines in the output
- C. Highlights only the command lines containing "badstring"
- D. Prevents command lines containing "badstring" from being displayed

Answer: D

Explanation:
In the Powershell Hunt report, the filtering condition of commandLine! ="badstring " prevents command lines containing "badstring" from being displayed. The ! operator is used to negate or exclude a condition from the search results. The * operator is used as a wildcard to match any number of characters before or after the specified string. Therefore, commandLine! ="badstring " means to filter out any command line that has "badstring" anywhere in it. The other options are not correct, as they do not describe what the filtering condition does.

NEW QUESTION # 62
Which of the following is a way to create event searches that run automatically and recur on a schedule that you set?

- A. Scheduled Searches
- B. Event Search
- C. Workflows
- D. Scheduled Reports

Answer: A

Explanation:
Scheduled Searches are a way to create event searches that run automatically and recur on a schedule that you set. You can use Scheduled Searches to monitor your environment for specific conditions or patterns, generate reports or alerts, or enrich your data with additional fields or tags. Workflows, Event Search, and Scheduled Reports are not ways to create event searches that run automatically and recur on a schedule.

NEW QUESTION # 63
What kind of activity does a User Search help you investigate?

- A. A count of failed user logon activity
- B. A list of process activity executed by the specified user account
- C. A list of DNS queries by the specified user account
- D. A history of Falcon Ul logon activity

Answer: B

Explanation:
User Search is an Investigate tool that helps you investigate a list of process activity executed by the specified user account. It shows information such as process name, command line, parent process name, parent command line, etc. for each process that was executed by the user account on any host in your environment. It does not show a history of Falcon UI logon activity, a count of failed user logon activity, or a list of DNS queries by the specified user account.

NEW QUESTION # 64
Which of the following is a suspicious process behavior?

- A. Non-network processes (eg, notepad exe) making an outbound network connection
- B. PowerShell running an execution policy of RemoteSigned
- C. An Internet browser (eg, Internet Explorer) performing multiple DNS requests
- D. PowerShell launching a PowerShell script

Answer: A

Explanation:
Non-network processes are processes that are not expected to communicate over the network, such as notepad.exe. If they make an outbound network connection, it could indicate that they are compromised or maliciously used by an adversary. PowerShell running an execution policy of RemoteSigned is a default setting that allows local scripts to run without digital signatures. An Internet browser performing multiple DNS requests is a normal behavior for web browsing. PowerShell launching a PowerShell script is also a common behavior for legitimate tasks.

NEW QUESTION # 65
.....

No matter how good the product is users will encounter some difficult problems in the process of use. Our CCFH-202b real exam materials are not exceptional also, in order to enjoy the best product experience, as long as the user is in use process found any problem, can timely feedback to us, for the first time you check our CCFH-202b Exam Question performance, professional maintenance staff to help users solve problems. Our CCFH-202b learning reference files have a high efficient product maintenance team, and they can send the CCFH-202b exam questions to you in a few minutes.

Hunter Exam Products □ Search for ☀ CCFH-202b □☀□ and download it for free immediately on ➤ www.pdfvce.com □ □CCFH-202b Reliable Test Sims

- Reliable CCFH-202b Test Voucher □ CCFH-202b Study Guide □ Certified CCFH-202b Questions □ ➥ www.verifieddumps.com □ is best website to obtain { CCFH-202b } for free download □CCFH-202b Study Guide
- CCFH-202b Reliable Exam Syllabus □ CCFH-202b Guaranteed Passing □ CCFH-202b Reliable Test Sample ～ Immediately open 《 www.pdfvce.com 》 and search for ➡ CCFH-202b □□□ to obtain a free download □CCFH-202b Reliable Exam Questions
- Free PDF 2026 CrowdStrike CCFH-202b: CrowdStrike Certified Falcon Hunter –Valid Exam Syllabus □ Download ➠ CCFH-202b □ for free by simply searching on ☀ www.exam4labs.com □☀□ □Practice Test CCFH-202b Pdf
- CCFH-202b Reliable Test Sample □ CCFH-202b Most Reliable Questions □ CCFH-202b Sample Questions □ Open ✔ www.pdfvce.com □✔□ and search for ➤ CCFH-202b □ to download exam materials for free □Latest CCFH-202b Exam Registration
- CCFH-202b Latest Braindumps □ CCFH-202b Guaranteed Passing ✡ Practice Test CCFH-202b Pdf □ Search for ➽ CCFH-202b □ on ➤ www.torrentvce.com □ immediately to obtain a free download □New CCFH-202b Exam Notes
- Pass Guaranteed CrowdStrike - CCFH-202b - Exam CrowdStrike Certified Falcon Hunter Syllabus □ Easily obtain [CCFH-202b] for free download through （ www.pdfvce.com ） □CCFH-202b Pass4sure Dumps Pdf
- Valid Exam CCFH-202b Syllabus Offers Candidates High Pass-rate Actual CrowdStrike CrowdStrike Certified Falcon Hunter Exam Products □ Download 「 CCFH-202b 」 for free by simply searching on ⇛ www.pass4test.com ⇚ □ □New CCFH-202b Braindumps Pdf
- bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes