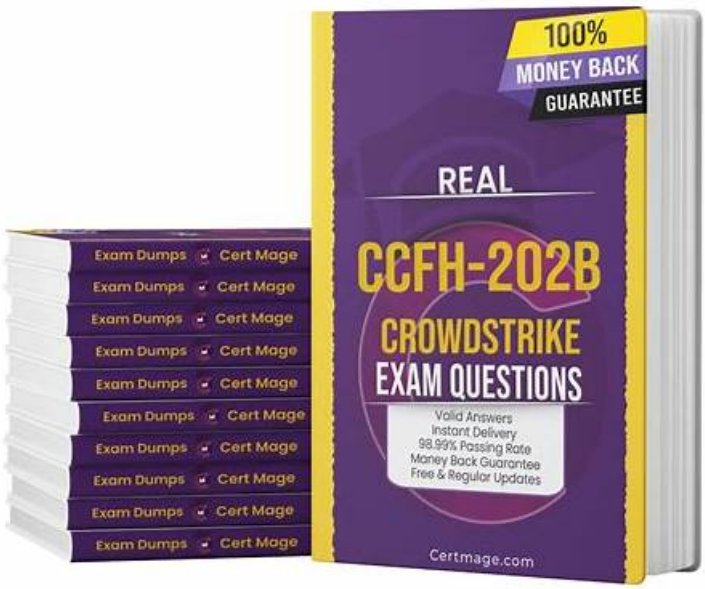
Reliable CCFH-202b Exam Pattern - CCFH-202b Valid Test Preparation



What's more, part of that DumpsValid CCFH-202b dumps now are free: https://drive.google.com/open?id=1BcBY2iELQzW0hXTtULvL-rZTG52pEwbe

By unremitting effort to improve the accuracy and being studious of the CCFH-202b real questions all these years, our experts remain unpretentious attitude towards our CCFH-202b practice materials all the time. They are unsuspecting experts who you can count on. Without unintelligible content within our CCFH-202b Study Tool, all questions of the exam are based on their professional experience in this industry. Besides, they made three versions for your reference, the PDF, APP and Online software version.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.
Topic 2	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
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.

>> Reliable CCFH-202b Exam Pattern <<

CCFH-202b Valid Test Preparation, CCFH-202b Valid Test Topics

DumpsValid has the ability to help IT people for success. DumpsValid CrowdStrike CCFH-202b exam dumps are the training

materials that help you succeed. As long as you want to Pass CCFH-202b Test, you must choose DumpsValid. We guarantee your success in the first attempt. If you fail, we will give you a FULL REFUND of your purchasing fee.

CrowdStrike Certified Falcon Hunter Sample Questions (Q13-Q18):

NEW QUESTION # 13
Which of the following is an example of a Falcon threat hunting lead?

- A. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories
- B. An external report describing a unique 5 character file extension for ransomware encrypted files
- C. A help desk ticket for a user clicking on a link in an email causing their machine to become unresponsive and have high CPU usage
- D. Security appliance logs showing potentially bad traffic to an unknown external IP address

Answer: A

Explanation:
A Falcon threat hunting lead is a piece of information that can be used to initiate or guide a threat hunting activity within the Falcon platform. A routine threat hunt query showing process executions of single letter filename (e.g., a.exe) from temporary directories is an example of a Falcon threat hunting lead, as it can indicate potential malicious activity that can be further investigated using Falcon data and features. Security appliance logs, help desk tickets, and external reports are not examples of Falcon threat hunting leads, as they are not directly related to the Falcon platform or data.

NEW QUESTION # 14
Which field in a DNS Request event points to the responsible process?

- A. ParentProcessId_decimal
- B. ContextProcessId_decimal
- C. ContextProcessId_readable
- D. TargetProcessId_decimal

Answer: C

Explanation:
The ContextProcessId_readable field in a DNS Request event points to the responsible process. The ContextProcessId_readable field is the readable representation of the process identifier for the process that initiated the DNS request. It can be used to identify which process was communicating with a specific domain or IP address. The TargetProcessId_decimal, ContextProcessId_decimal, and ParentProcessId_decimal fields do not point to the responsible process.

NEW QUESTION # 15
While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS "
What does this User Name indicate?

- A. The Falcon sensor could not determine the User Name
- B. The User Name is a System User
- C. The User Name is not relevant for the dashboard
- D. There is no User Name associated with the event

Answer: D

Explanation:
When you see "hostnameS" in the User Name column in the Host Search page, it means that there is no User Name associated with the event. This can happen when the event is related to a system process or service that does not have a user context. It does not mean that the User Name is a System User, that the User Name is not relevant for the dashboard, or that the Falcon sensor could not determine the User Name.

NEW QUESTION # 16

What Investigate tool would you use to allow an analyst to view all events for a specific host?

- A. Process Timeline
- B. Bulk Timeline
- C. Host Timeline
- D. Host Search

Answer: C

Explanation:
The Host Timeline is the Investigate tool that you would use to allow an analyst to view all events for a specific host. The Host Timeline shows a graphical representation of all events that occurred on a host within a specified time range. It allows an analyst to zoom in and out, filter by event type or name, and drill down into event details. The Bulk Timeline, the Host Search, and the Process Timeline are not Investigate tools that you would use to view all events for a specific host.

NEW QUESTION # 17
Lateral movement through a victim environment is an example of which stage of the Cyber Kill Chain?

- A. Actions on Objectives
- B. Delivery
- C. Command & Control
- D. Exploitation

Answer: C

Explanation:
Lateral movement through a victim environment is an example of the Command & Control stage of the Cyber Kill Chain. The Cyber Kill Chain is a model that describes the phases of a cyber attack, from reconnaissance to actions on objectives. The Command & Control stage is where the adversary establishes and maintains communication with the compromised systems and moves laterally to expand their access and control.

NEW QUESTION # 18
.....

□New CCFH-202b Test Labs

- Reliable CCFH-202b Test Question □ CCFH-202b Test Prep □ CCFH-202b Latest Real Exam □ Open ⇛ www.dumpsmaterials.com ⇚ enter ⇛ CCFH-202b ⇚ and obtain a free download □CCFH-202b Examcollection Dumps Torrent
- CCFH-202b Examcollection Dumps Torrent □ CCFH-202b Exam Collection Pdf □ CCFH-202b Braindumps Torrent □ □ Simply search for ▸ CCFH-202b ◂ for free download on 「 www.pdfvce.com 」 □CCFH-202b Test Prep
- Ace Your Exam with www.examcollectionpass.com CrowdStrike CCFH-202b Desktop Practice Test Software □ Search for 【 CCFH-202b 】 and obtain a free download on ➠ www.examcollectionpass.com □ □Reliable CCFH-202b Exam Sample
- janazizj730284.iyublog.com, luludnsc354161.blogsidea.com, gen-directory.com, privatebookmark.com, www.stes.tyc.edu.tw, umairmbmp106770.tdlwiki.com, redhotbookmarks.com, directoryhere.com, bookmarkforest.com, ihannavjqb595234.activablog.com, Disposable vapes

BTW, DOWNLOAD part of DumpsValid CCFH-202b dumps from Cloud Storage: https://drive.google.com/open?id=1BcBY2iELQzW0hXTtULvL-rZTG52pEwbe