CrowdStrike CCFH-202b Practice Mock & Study CCFH-202b Center

For a company with history more than ten years, our CCFH-202b practice materials have developed into fully academic maturity. All content are arranged legibly. There are three kinds of CCFH-202b exam braindumps for your reference: the PDF, the Software and the APP online. All these versions of our CCFH-202b study questions are high-efficient. You can choose either one in accordance with your interests or habits.

Normally, you just need to wait for about five to ten minutes after you purchase our CCFH-202b learning braindumps. If you do not receive our CCFH-202b study materials, please contact our online workers. It is our great advantage to attract customers. In a word, our running efficiency on CCFH-202b Exam Questions is excellent. Time is priceless. Once you receive our email, just begin to your new learning journey.

>> CrowdStrike CCFH-202b Practice Mock <<

Study CCFH-202b Center, Valid CCFH-202b Exam Cost

The CrowdStrike CCFH-202b is so flexible that you can easily change the timings, types of questions, and topics for each mock exam.CrowdStrike CCFH-202b practice test contains all the important questions that will appear in the actual CCFH-202b Exam. PDFDumps offers updates for CrowdStrike CCFH-202b Exam questions up to 365 days after purchase, to match the changes in the latest CCFH-202b exam syllabus.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	- Hunting Analytics: This domain focuses on recognizing malicious behaviors, evaluating information reliability, decoding command line activity, identifying infection patterns, distinguishing legitimate from adversary activity, and identifying exploited vulnerabilities.
Topic 2	- 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 3	- 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 4	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.

CrowdStrike Certified Falcon Hunter Sample Questions (Q59-Q64):

NEW QUESTION # 59
In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

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

Answer: C

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 # 60
With Custom Alerts you are able to configure email alerts using predefined templates so you're notified about specific activity in your environment. Which of the following outlines the steps required to properly create a custom alert rule?

- A. Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert
- B. Create a new custom template, configure the email template, and then create the custom query for the alert
- C. Choose the template you would like to configure, preview the search results, and then schedule the alert
- D. Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert

Answer: C

Explanation:
These are the steps required to properly create a custom alert rule. Custom Alerts are a feature that allows you to configure email alerts using predefined templates so you're notified about specific activity in your environment. You can choose from various templates that cover different use cases, such as suspicious PowerShell activity, network connections to risky countries, etc. You can also preview the search results of the template before scheduling the alert. You do not need to create the query for the alert, setup the email template for the alert, or create a new custom template, as these are already provided by the predefined templates.

NEW QUESTION # 61
What Investigate tool would you use to allow an analyst to view all events for a specific host?

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

Answer: D

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 # 62
What information is provided when using IP Search to look up an IP address?

- A. Suspicious IP addresses
- B. Internal IPs only
- C. Both internal and external IPs
- D. External IPs only

Answer: D

Explanation:
IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.

NEW QUESTION # 63
What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

- A. CID
- B. Process ID or Parent Process ID
- C. PID
- D. Process Timeline Link

Answer: D

Explanation:
The Process Timeline Link is what you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search. The Process Timeline Link is an icon that looks like three horizontal bars with dots on them. It appears next to each process name or ID on various pages in Falcon, such as Hash Search results, Detection details, Event Search results, etc. Clicking on it will open a new tab with the Process Timeline for that process. The PID, the Process ID or Parent Process ID, and the CID are not what you click to jump to a Process Timeline.

NEW QUESTION # 64
......

In order to ensure that the examinees in the CCFH-202b exam certification make good achievements, our PDFDumps has always been trying our best. With efforts for years, the passing rate of PDFDumps's CCFH-202b certification exam has reached as high as 100%. After you purchase our CCFH-202b Exam Training materials, if there is any quality problem or you fail CCFH-202b exam certification, we promise to give a full refund unconditionally.

Study CCFH-202b Center: https://www.pdfdumps.com/CCFH-202b-valid-exam.html and download it for free on ⇛ www.verifieddumps.com ⇚ website □Latest CCFH-202b Exam Tips

- CCFH-202b Free Practice Exams □ CCFH-202b Cert Exam □ CCFH-202b Flexible Learning Mode □ Easily obtain ☀ CCFH-202b □☀□ for free download through ➠ www.pdfvce.com □ □Valid Braindumps CCFH-202b Book
- CCFH-202b PDF Questions □ CCFH-202b Flexible Learning Mode □ CCFH-202b Exam Simulator Online □ Search for ▸ CCFH-202b ◂ and easily obtain a free download on { www.easy4engine.com } □CCFH-202b PDF Questions
- CCFH-202b Exam Simulator Online □ Latest CCFH-202b Exam Tips □ CCFH-202b Reliable Exam Simulations □ Search for ▸ CCFH-202b ◂ and download it for free on ➠ www.pdfvce.com □ website ↘ Real CCFH-202b Question
- Real CCFH-202b Question □ Valid Braindumps CCFH-202b Book □ CCFH-202b Exam Simulator Online □ Search for ⇛ CCFH-202b ⇚ and download exam materials for free through （ www.pass4test.com ） □Flexible CCFH-202b Testing Engine
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes