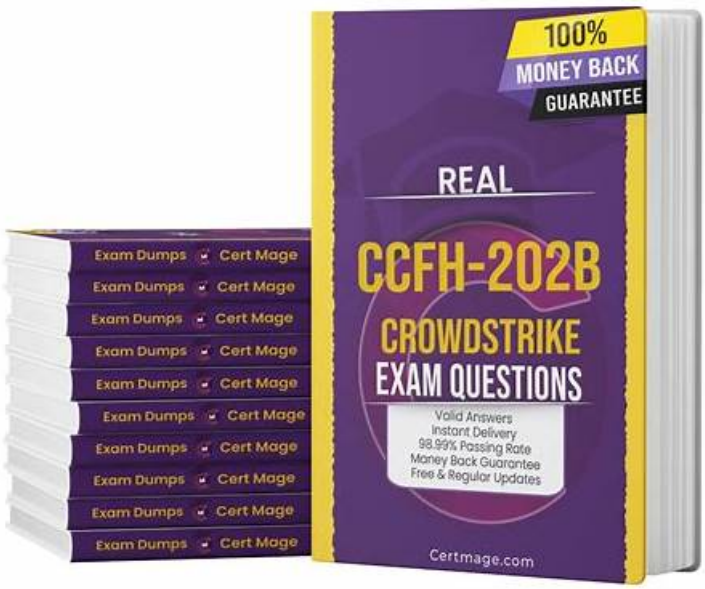
Real CCFH-202b Exam Questions & CCFH-202b Test Discount Voucher



P.S. Free & New CCFH-202b dumps are available on Google Drive shared by Dumps4PDF: https://drive.google.com/open?id=1OatfGZcPwj15QexfJBdpih6bT8hasLcI

Are you looking for valid IT exam materials or study guide? You can try our free CrowdStrike CCFH-202b new exam collection materials. We offer free demo download for our PDF version. You can know several questions of the real test. It can make you master fundamental knowledge quickly. Our CCFH-202b new exam collection materials are authorized legal products. Our accuracy is nearly 100% pass which will help you clear exam.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 2	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
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	• 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 5	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.

>> Real CCFH-202b Exam Questions <<

CCFH-202b Test Discount Voucher, CCFH-202b Pdf Version

They can try a free demo for satisfaction before buying our CrowdStrike CCFH-202b dumps. And a 24/7 support system assists them whenever they are stuck in any problem or issue. This CrowdStrike Certified Falcon Hunter (CCFH-202b) questions is a complete package and a blessing for candidates who want to prepare quickly for the CCFH-202b exam. Buy It Now!

CrowdStrike Certified Falcon Hunter Sample Questions (Q41-Q46):

NEW QUESTION # 41
In the Powershell Hunt report, what does the filtering condition of commandLine! ="*badstring* " do?

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

Answer: B

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 # 42
Which pre-defined reports offer information surrounding activities that typically indicate suspicious activity occurring on a system?

- A. Scheduled searches
- B. Hunt reports
- C. Timeline reports
- D. Sensor reports

Answer: B

Explanation:
Hunt reports are pre-defined reports that offer information surrounding activities that typically indicate suspicious activity occurring on a system. They are based on common threat hunting use cases and queries, and they provide visualizations and summaries of the results. Hunt reports can help threat hunters quickly identify and investigate potential threats in their environment.

NEW QUESTION # 43
What elements are required to properly execute a Process Timeline?

- A. Agent ID (AID) only
- B. Target Process ID only
- C. Hostname and Local Process ID
- D. Agent ID (AID) and Target Process ID

Answer: D

Explanation:
The Agent ID (AID) and the Target Process ID are the elements that are required to properly execute a Process Timeline. The Agent ID (AID) is a unique identifier for each host that has a Falcon sensor installed. The Target Process ID is the decimal representation of the process identifier for the process that you want to investigate. These two elements are used to query the cloud for the events related to the process on the host. The Agent ID (AID) only, the Hostname and Local Process ID, and the Target Process ID only are not sufficient to execute a Process Timeline.

NEW QUESTION # 44
What is the difference between a Host Search and a Host Timeline?

- A. 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
- B. Host Search is used for detection investigation and Host Timeline is used for proactive hunting
- C. There is no difference. You just get to them different ways
- D. 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

Answer: A

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 # 45
Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

- A. Competitive analysis
- B. Model hunting framework
- C. Key assumptions check
- D. Analysis of competing hypotheses

Answer: D

Explanation:
Analysis of competing hypotheses is a structured analytic technique that contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis. It involves listing all the possible hypotheses, identifying the evidence and assumptions for each hypothesis, evaluating the consistency and reliability of the evidence and assumptions, and rating the likelihood of each hypothesis based on the evidence and assumptions.

NEW QUESTION # 46
.....

www.pdfvce.com ◂ is best website to obtain ▸ CCFH-202b ◂ for free download □CCFH-202b Unlimited Exam Practice

- CrowdStrike CCFH-202b Exam is Easy with Our Valid Real CCFH-202b Exam Questions: CrowdStrike Certified Falcon Hunter Certainly □ Search for ☀ CCFH-202b □☀□ and easily obtain a free download on 【 www.troytecdumps.com 】 □CCFH-202b Valid Test Cost
- Latest CCFH-202b Exam Cram □ CCFH-202b Latest Test Answers □ CCFH-202b Valid Dumps Ppt □ Enter [www.pdfvce.com] and search for " CCFH-202b " to download for free □CCFH-202b Exam Question
- CCFH-202b Exam Questions - CrowdStrike Certified Falcon Hunter Exam Tests - CCFH-202b Test Guide □ Search for ➽ CCFH-202b □ and obtain a free download on ➥ www.examcollectionpass.com □ □CCFH-202b Valid Test Simulator
- Relevant CCFH-202b Exam Dumps □ Demo CCFH-202b Test ✡ Relevant CCFH-202b Exam Dumps □ Search on □ www.pdfvce.com □ for ➡ CCFH-202b □□□ to obtain exam materials for free download □CCFH-202b New Dumps
- Free CCFH-202b Pdf Guide □ Latest CCFH-202b Dumps Ebook □ CCFH-202b Braindump Pdf □ Enter □ www.validtorrent.com □ and search for ☀ CCFH-202b □☀□ to download for free □CCFH-202b Latest Dumps Ebook
- academy.quantalgos.in, amanchopra.net, sairapxza817324.snack-blog.com, topsocialplan.com, lewisglcl720093.wikiconversation.com, montymvqc212836.blogunteer.com, bookmarkspecial.com, thesocialintro.com, 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, liviagjvr341807.wikiworldstock.com, Disposable vapes

DOWNLOAD the newest Dumps4PDF CCFH-202b PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1OatfGZcPwj15QexfJBdpih6bT8hasLcI