Hot CrowdStrike CCFH-202b Online Test Are Leading Materials & Fast Download CCFH-202b Test Duration

P.S. Free & New CCFH-202b dumps are available on Google Drive shared by Prep4cram: https://drive.google.com/open?id=1WPTaaBud4ugMFM_IKNSdYQ2J-hBtIeKq

The Exams is committed to making the CrowdStrike CCFH-202b exam dumps the best CCFH-202b exam study material. To achieve this objective the Exams have hired a team of experienced and qualified CrowdStrike CCFH-202b Exam trainers. They work together and check all CrowdStrike CCFH-202b exam questions step by step and ensure the top standard of CrowdStrike CCFH-202b practice test material all the time.

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	• 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 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.

>> CCFH-202b Online Test <<

Achieve your goals with CCFH-202b actual dumps & CrowdStrike CCFH-202b exam pdf

We all know that pass the CCFH-202b exam will bring us many benefits, but it is not easy for every candidate to achieve it. The CCFH-202b guide torrent is a tool that aimed to help every candidate to pass the exam. Our CCFH-202b exam materials can installation and download set no limits for difficulty of the computers and persons. You can use our CCFH-202b Practice Questions directly. We guarantee you that the CCFH-202b study materials we provide to you are useful and can help you pass the test.

CrowdStrike Certified Falcon Hunter Sample Questions (Q40-Q45):

NEW QUESTION # 40
What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

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

Answer: A

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 # 41
Which of the following is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain?

- A. Loading a malicious payload into a common DLL
- B. Emailing the intended victim with a malware attachment
- C. Installing a backdoor on the victim endpoint
- D. Discovering internet-facing servers

Answer: D

Explanation:
Discovering internet-facing servers is an example of actor actions during the RECONNAISSANCE phase of the Cyber Kill Chain. The RECONNAISSANCE phase is where the adversary researches and identifies targets, vulnerabilities, and attack vectors. Discovering internet-facing servers is a way for the adversary to find potential entry points or weaknesses in the target network.

NEW QUESTION # 42
Which field should you reference in order to find the system time of a *FileWritten event?

- A. ProcessStartTime_decimal
- B. timestamp
- C. FileTimeStamp_decimal
- D. ContextTimeStamp_decimal

Answer: D

Explanation:
ContextTimeStamp_decimal is the field that shows the system time of the event that triggered the sensor to send data to the cloud. In this case, it would be the time when the file was written. FileTimeStamp_decimal is the field that shows the last modified time of the file, which may not be the same as the time when the file was written. ProcessStartTime_decimal is the field that shows the start time of the process that performed the file write operation, which may not be the same as the time when the file was written. Timestamp is the field that shows the time when the sensor data was received by the cloud, which may not be the same as the time when the file was written.

NEW QUESTION # 43
Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

- A. MITRE ATT&CK
- B. Lockheed Martin Cyber Kill Chain
- C. NIST 800-171 Cyber Threat Framework
- D. Director of National Intelligence Cyber Threat Framework

Answer: A

Explanation:
MITRE ATT&CK is a threat framework that allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies. It is a knowledge base of adversary behaviors and tactics that covers various platforms, domains, and scenarios. It provides a common language and structure for threat hunters to understand and analyze threats, as well as to share findings and recommendations.

NEW QUESTION # 44
What is the main purpose of the Mac Sensor report?

- A. To provide vulnerability assessment for Mac Operating Systems
- B. To provide a summary view of selected activities on Mac hosts
- C. To identify endpoints that are in Reduced Functionality Mode
- D. To provide a dashboard for Mac related detections

Answer: B

Explanation:
The Mac Sensor report is a pre-defined report that provides a summary view of selected activities on Mac hosts. It shows information such as process execution events, network connection events, file write events, etc. that occurred on Mac hosts within a specified time range. The Mac Sensor report does not identify endpoints that are in Reduced Functionality Mode, provide vulnerability assessment for Mac Operating Systems, or provide a dashboard for Mac related detections.

NEW QUESTION # 45
.....

Free domo will be provided for CCFH-202b study materials, and you can know deeper what you will buy. We offer you free update for 365 days after you purchasing. And the latest version will be sent to your email address automatically. Therefore you can get the latest information of the CCFH-202b Exam Dumps. Besides, we have the technicians to examine the website at times, and it will provide you with a clean and safe shopping environment. You just need to buy CCFH-202b study materials with ease.

CCFH-202b Test Duration: https://www.prep4cram.com/CCFH-202b_exam-questions.html

- Reliable CCFH-202b Test Review □ Reliable CCFH-202b Test Review □ CCFH-202b Authorized Pdf □ The page for free download of ➤ CCFH-202b □ on （ www.exam4labs.com ） will open immediately □Study CCFH-202b Demo
- CCFH-202b Test Lab Questions ～ CCFH-202b Reliable Test Question ☃ CCFH-202b Exam Review □ Search on □ www.pdfvce.com □ for ⇛ CCFH-202b ⇚ to obtain exam materials for free download □CCFH-202b Certification Exam
- CrowdStrike CCFH-202b Practice Exam (Desktop - Web-Based) □ Download [CCFH-202b] for free by simply searching on ▸ www.dumpsmaterials.com ◂ □Test CCFH-202b Free
- CrowdStrike CCFH-202b Practice Exam (Desktop - Web-Based) □ Search for ⇛ CCFH-202b ⇚ and obtain a free download on □ www.pdfvce.com □ □CCFH-202b Exam Review
- Free CCFH-202b Pdf Guide ⤴ CCFH-202b Reliable Exam Price □ CCFH-202b Reliable Test Question □ Search for ➤ CCFH-202b □ and easily obtain a free download on 「 www.troytecdumps.com 」 □Reliable Exam CCFH-202b Pass4sure
- Reliable CCFH-202b Exam Review ⧖ CCFH-202b Authorized Pdf □ Reliable CCFH-202b Test Review □ Open ☀ www.pdfvce.com □☀□ and search for 【 CCFH-202b 】 to download exam materials for free □CCFH-202b Vce Torrent
- Free CCFH-202b Pdf Guide □ CCFH-202b Reliable Exam Price □ Valid CCFH-202b Test Topics □ Enter ▹

www.testkingpass.com◁ and search for 「 CCFH-202b 」 to download for free □Reliable Exam CCFH-202b Pass4sure

- Excellent CCFH-202b Online Test - Win Your CrowdStrike Certificate with Top Score □ Open ✔ www.pdfvce.com □✔□ and search for ✔ CCFH-202b □✔□ to download exam materials for free □CCFH-202b Reliable Exam Syllabus
- Excellent CCFH-202b Online Test - Win Your CrowdStrike Certificate with Top Score □ Search for ▸ CCFH-202b ◂ and easily obtain a free download on ➤ www.vce4dumps.com □ □Valid CCFH-202b Test Topics
- Test CCFH-202b Free □ CCFH-202b Test Lab Questions □ CCFH-202b Authorized Pdf □ Easily obtain free download of【 CCFH-202b 】 by searching on ▸ www.pdfvce.com ◂ □CCFH-202b Reliable Test Sims
- Pass Guaranteed Quiz CCFH-202b - CrowdStrike Certified Falcon Hunter Updated Online Test □ Open ✔ www.vce4dumps.com □✔□ and search for （ CCFH-202b ） to download exam materials for free □Valid CCFH-202b Test Topics
- socialrator.com, www.notebook.ai, sairatgip929176.fliplife-wiki.com, stevedzvx694024.blogsumer.com, p.me-page.com, userbookmark.com, ianmhwv382016.wikitron.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, myportal.utt.edu.tt, agnestdka798050.dailyblogzz.com, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CCFH-202b dumps are available on Google Drive shared by Prep4cram: https://drive.google.com/open?id=1WPTaaBud4ugMFM_IKNSdYQ2J-hBtIeKq