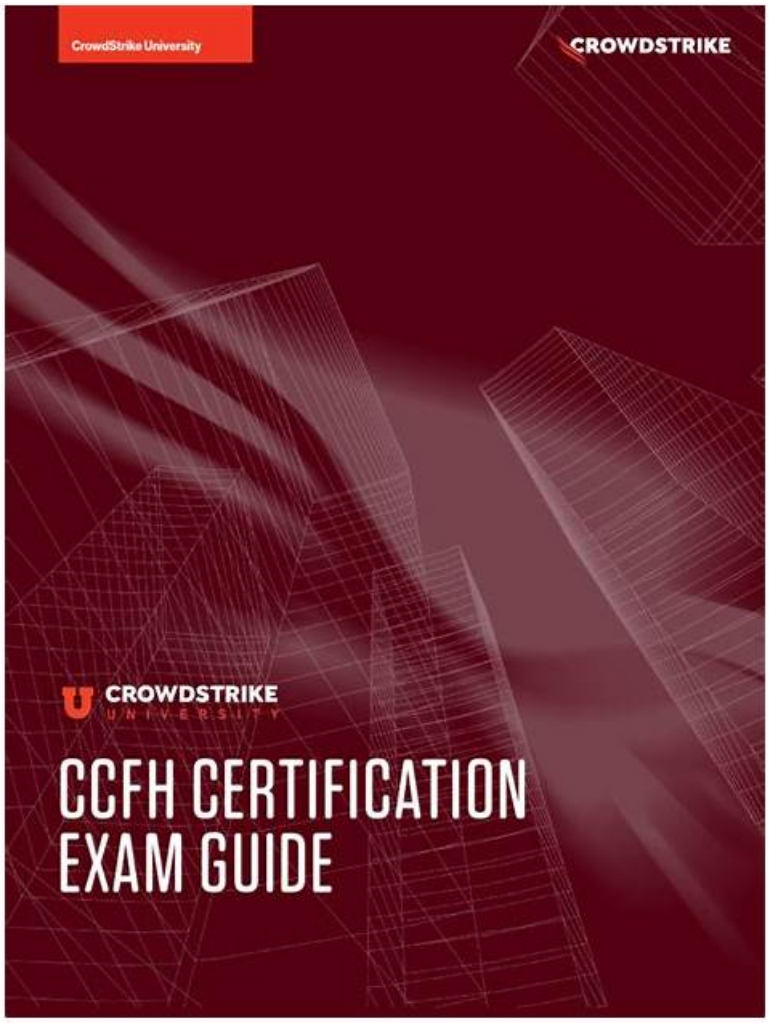
CCFH-202b Valid Exam Questions - CCFH-202b Test Guide Online



As is known to us, our company has promised that the CCFH-202b exam braindumps from our company will provide more than 99% pass guarantee for all people who try their best to prepare for the exam. If you are preparing for the exam by the guidance of the CCFH-202b study practice question from our company and take it into consideration seriously, you will absolutely pass the exam and get the related certification. So do not hesitate and hurry to buy our study materials.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 2	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
Topic 3	• 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 4	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.

Topic 5	• 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 6	• 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 Test Guide Online, CCFH-202b Reliable Learning Materials

We provide 24-hours online customer service which replies the client's questions and doubts about our CCFH-202b training quiz and solve their problems. Our professional personnel provide long-distance assistance online. If the clients can't pass the CCFH-202b Exam we will refund them immediately in full at one time. So there is nothing to worry about our CCFH-202b exam questions. And it is totally safe to buy our CCFH-202b learning guide.

CrowdStrike Certified Falcon Hunter Sample Questions (Q22-Q27):

NEW QUESTION # 22
Which structured analytic technique contrasts different hypotheses to determine which is the best leading (prioritized) hypothesis?

- A. Key assumptions check
- B. Model hunting framework
- C. Competitive analysis
- 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 # 23
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. NIST 800-171 Cyber Threat Framework
- C. Lockheed Martin Cyber Kill Chain
- 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 # 24
When performing a raw event search via the Events search page, what are Event Actions?

- A. Event Actions contains the summary of actions taken by the Falcon sensor such as quarantining a file, prevent a process

from executing or taking no actions and creating a detection only

- B. Event Actions are pivotable workflows including connecting to a host, pre-made event searches and pivots to other investigatory pages such as host search
- C. Event Actions contains an audit information log of actions an analyst took in regards to a specific detection
- D. Event Actions is the field name that contains the event name defined in the Events Data Dictionary such as ProcessRollup, SyntheticProcessRollup, DNS request, etc

Answer: B

Explanation:
When performing a raw event search via the Events search page, Event Actions are pivotable workflows that allow you to perform various tasks related to the event or the host. For example, you can connect to a host using Real Time Response, run pre-made event searches based on the event type or name, or pivot to other investigatory pages such as host search, hash search, etc. Event Actions do not contain audit information log, summary of actions taken by the Falcon sensor, or the event name defined in the Events Data Dictionary.

NEW QUESTION # 25
Lateral movement through a victim environment is an example of which stage of the Cyber Kill Chain?

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

Answer: A

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 # 26
Adversaries commonly execute discovery commands such as netexe, ipconfig.exe, and whoami exe. Rather than query for each of these commands individually, you would like to use a single query with all of them. What Splunk operator is needed to complete the following query?

- A. OR
- B. IN
- C. NOT
- D. AND

Answer: A

Explanation:
The OR operator is needed to complete the following query, as it allows to search for events that match any of the specified values. The query would look like this:
event_simpleName=ProcessRollup2 FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe The OR operator is used to combine multiple search terms or expressions and return events that match at least one of them. The IN, NOT, and AND operators are not suitable for this query, as they have different functions and meanings.

NEW QUESTION # 27
.....

CCFH-202b Test Guide Online: https://www.vce4dumps.com/CCFH-202b-valid-torrent.html

- CrowdStrike CCFH-202b Exam is Easy with Our Reliable CCFH-202b Valid Exam Questions: CrowdStrike Certified Falcon Hunter Efficiently □ Immediately open { www.practicevce.com } and search for { CCFH-202b } to obtain a free download □Latest CCFH-202b Test Dumps
- CCFH-202b Test Book □ CCFH-202b New Dumps Sheet □ CCFH-202b Exam Cost ✏ Search for [CCFH-202b] and download exam materials for free through ▷ www.pdfvce.com ◁ ☢Latest CCFH-202b Test Dumps
- CCFH-202b Exam Cost □ CCFH-202b Exam Cost □ CCFH-202b New Dumps Sheet □ Search for ➽ CCFH-202b □ on （ www.validtorrent.com ） immediately to obtain a free download □CCFH-202b Exam Braindumps
- CCFH-202b Latest Dumps Free □ Latest CCFH-202b Test Dumps □ CCFH-202b New Dumps Sheet □ Search on ➠ www.pdfvce.com □ for ▶ CCFH-202b ◀ to obtain exam materials for free download ↪Reliable CCFH-202b Study Plan
- Practical CCFH-202b Valid Exam Questions | Amazing Pass Rate For CCFH-202b Exam | Valid CCFH-202b: CrowdStrike Certified Falcon Hunter □ Search for 《 CCFH-202b 》 and download it for free on ➥ www.prep4away.com □ website □CCFH-202b New Dumps Sheet
- 100% Pass Quiz CCFH-202b - The Best CrowdStrike Certified Falcon Hunter Valid Exam Questions □ Search on ➽ www.pdfvce.com □ for ▶ CCFH-202b ◀ to obtain exam materials for free download □Best CCFH-202b Preparation Materials
- Quiz CrowdStrike - Fantastic CCFH-202b Valid Exam Questions □ Search for 「 CCFH-202b 」 and download it for free immediately on ▷ www.prep4away.com ◁ □CCFH-202b Exam Braindumps
- 2026 Accurate CrowdStrike CCFH-202b: CrowdStrike Certified Falcon Hunter Valid Exam Questions □ Easily obtain 「 CCFH-202b 」 for free download through ▶ www.pdfvce.com ◀ □CCFH-202b Training Material
- Practical CCFH-202b Valid Exam Questions | Amazing Pass Rate For CCFH-202b Exam | Valid CCFH-202b: CrowdStrike Certified Falcon Hunter □ Easily obtain free download of 《 CCFH-202b 》 by searching on ➠ www.vceengine.com □ □CCFH-202b Actual Questions
- CCFH-202b Brain Exam □ CCFH-202b Clearer Explanation □ CCFH-202b Exam Cost □ Search for （ CCFH-202b ） and easily obtain a free download on ➥ www.pdfvce.com □ □CCFH-202b Latest Dumps Free
- CCFH-202b New Dumps Sheet □ Reliable CCFH-202b Study Plan □ CCFH-202b New Dumps Sheet □ Simply search for 《 CCFH-202b 》 for free download on ✔ www.pdfdumps.com □✔□ □Latest CCFH-202b Test Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, aavitechveda.com, hhi.instructure.com, www.notebook.ai, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, Disposable vapes