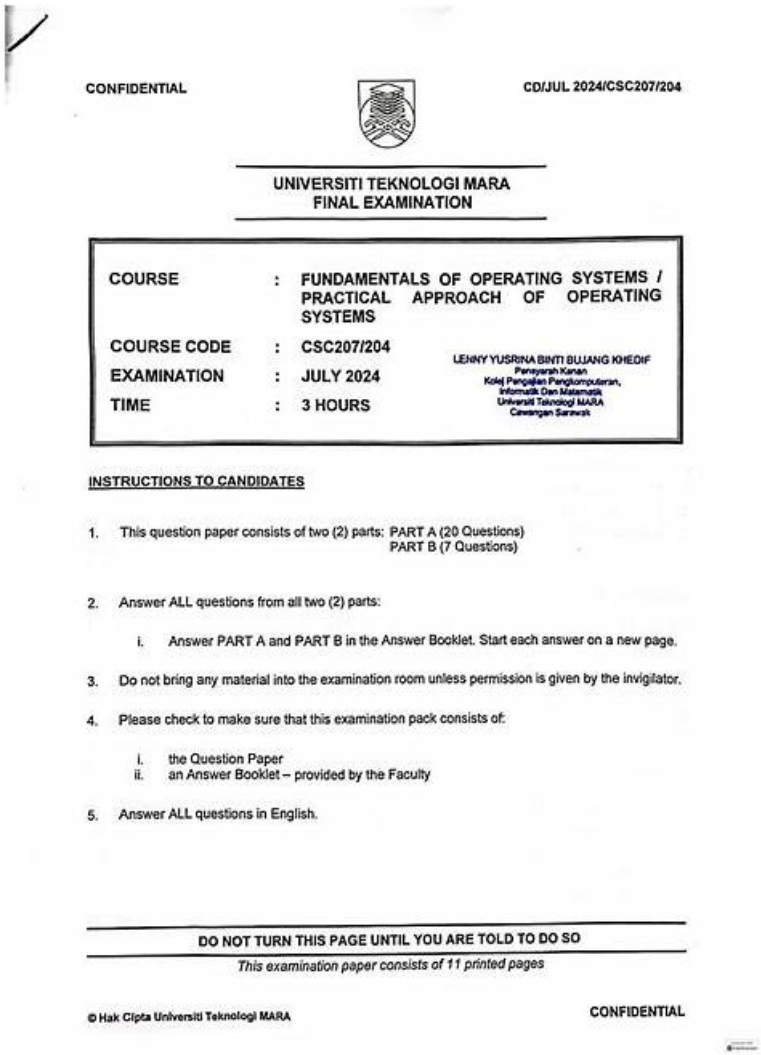
CCFH-202b Practice Questions | Best CCFH-202b Practice



CONFIDENTIAL

CD/JUL 2024/CSC207/204

UNIVERSITI TEKNOLOGI MARA
FINAL EXAMINATION

COURSE	:	FUNDAMENTALS OF OPERATING SYSTEMS / PRACTICAL APPROACH OF OPERATING SYSTEMS
COURSE CODE	:	CSC207/204
EXAMINATION	:	JULY 2024
TIME	:	3 HOURS

LENNY YUSRINA BINTI BUJANG KHEDIF
Pensyarah Kanan
Kolej Pengajian Pengkomputeran,
Informatik Dan Matematik
Universiti Teknologi MARA
Cawangan Sarawak

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of two (2) parts: PART A (20 Questions)
   PART B (7 Questions)
2. Answer ALL questions from all two (2) parts:
   i. Answer PART A and PART B in the Answer Booklet. Start each answer on a new page.
3. Do not bring any material into the examination room unless permission is given by the invigilator.
4. Please check to make sure that this examination pack consists of:
   i. the Question Paper
   ii. an Answer Booklet – provided by the Faculty
5. Answer ALL questions in English.

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

This examination paper consists of 11 printed pages

CONFIDENTIAL

DOWNLOAD the newest ActualTestsQuiz CCFH-202b PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1P5IM0uK5ZR_jRnrvcEKKK5cVqhDjGsUd

Taking ActualTestsQuiz CrowdStrike Certified Falcon Hunter (CCFH-202b) practice test questions are also important. These CCFH-202b practice exams include questions that are based on a similar pattern as the finals. This makes it easy for the candidates to understand the CrowdStrike Certified Falcon Hunter (CCFH-202b) exam question paper and manage the time. It is indeed a booster for the people who work hard and do not want to leave any chance of clearing the CCFH-202b Exam with brilliant scores. These CrowdStrike Certified Falcon Hunter (CCFH-202b) practice test questions also boost your confidence.

The procedures of every step to buy our CCFH-202b exam questions are simple and save the clients' time. Because the most clients may be busy in their jobs or other significant things, the time they can spare to learn our CCFH-202b study materials is limited and little. But if the clients buy our CCFH-202b training quiz they can immediately use our exam products and save their time. It will only take 5 to 10 minutes for us to send the CCFH-202b learning guide to you after purchase.

>> CCFH-202b Practice Questions <<

CCFH-202b Question Dumps Keep the High Accuracy of CrowdStrike Certified Falcon Hunter Exam - ActualTestsQuiz

Our ActualTestsQuiz website try our best for the majority of examinees to provide the best and most convenient service. Under the joint efforts of everyone for many years, the passing rate of ActualTestsQuiz CrowdStrike's CCFH-202b Certification Exam has reached as high as100%. If you buy our CCFH-202b exam certification training materials, we will also provide one year free renewal service. Hurry up!

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	• 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	• 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.
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	• 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.

CrowdStrike Certified Falcon Hunter Sample Questions (Q54-Q59):

NEW QUESTION # 54
What Investigate tool would you use to allow an analyst to view all events for a specific host?

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

Answer: A

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 # 55
What information is provided from the MITRE ATT&CK framework in a detection's Execution Details?

- A. Command Line
- B. Technique ID
- C. Triggering Indicator
- D. Grouping Tag

Answer: B

Explanation:

Technique ID is the information that is provided from the MITRE ATT&CK framework in a detection's Execution Details. Technique ID is a unique identifier for each technique in the MITRE ATT&CK framework, such as T1059 for Command and Scripting Interpreter or T1566 for Phishing. Technique ID helps to map a detection to a specific adversary behavior and tactic. Grouping Tag, Command Line, and Triggering Indicator are not information that is provided from the MITRE ATT&CK framework in a detection's Execution Details.

NEW QUESTION # 56
In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

- A. Weaponization
- B. Command & control
- C. Exploitation
- D. Installation

Answer: A

Explanation:
Weaponization is the stage of the Cyber Kill Chain where the actor does not interact with the victim endpoint(s). Weaponization is where the actor prepares or packages the exploit or payload that will be used to compromise the target. This stage does not involve any communication or interaction with the victim endpoint(s), as it is done by the actor before delivering the weaponized content. Exploitation, Command & Control, and Installation are all stages where the actor interacts with the victim endpoint(s), either by executing code, establishing communication, or installing malware.

NEW QUESTION # 57
What topics are presented in the Hunting and Investigation Guide?

- A. Sample hunting queries, select walkthroughs and best practices for hunting with Falcon
- B. Recommended platform configurations and prevention settings to ensure detections are generated for hunting leads
- C. Detailed summary of event names, descriptions, and some key data fields for hunting and investigation
- D. Detailed tutorial on writing advanced queries such as sub-searches and joins

Answer: A

Explanation:
This is the correct answer for the same reason as above. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It does not provide a detailed tutorial on writing advanced queries, a detailed summary of event names and descriptions, or recommended platform configurations and prevention settings.

NEW QUESTION # 58
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. Create a new custom template, configure the email template, and then create the custom query for the alert
- B. Choose the template you would like to configure, preview the search results, and then schedule the alert
- C. Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert
- D. Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert

Answer: B

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 # 59

.....

In modern society, everything is changing so fast with the development of technology. If you do no renew your knowledge and skills, you will be wiped out by others. Our CCFH-202b study materials also keep up with the society. After all, new technology has been applied in many fields. It is time to strengthen your skills. Our CCFH-202b Study Materials will help you master the most popular skills in the job market. Then you will have a greater chance to find a desirable job. Also, it doesn't matter whether have basic knowledge about the CCFH-202b study materials.

Best CCFH-202b Practice: https://www.actualtestsquiz.com/CCFH-202b-test-torrent.html

- 100% Pass 2026 CCFH-202b: CrowdStrike Certified Falcon Hunter –The Best Practice Questions □ Download ➤ CCFH-202b □ for free by simply searching on （ www.pdfdumps.com ） □New CCFH-202b Exam Notes
- Smashing CCFH-202b Guide Materials: CrowdStrike Certified Falcon Hunter Deliver You Unique Exam Braindumps - Pdfvce □ ▸ www.pdfvce.com ◂ is best website to obtain ▹ CCFH-202b ◃ for free download □CCFH-202b Valid Exam Cost
- Free PDF 2026 CrowdStrike Latest CCFH-202b: CrowdStrike Certified Falcon Hunter Practice Questions □ Search for ▸ CCFH-202b ◂ and download it for free immediately on 《 www.examdiscuss.com 》 □Practice Test CCFH-202b Fee
- 100% Pass 2026 CCFH-202b: CrowdStrike Certified Falcon Hunter –The Best Practice Questions □ Search for { CCFH-202b } and download it for free immediately on （ www.pdfvce.com ） □Valid CCFH-202b Practice Materials
- Exam CCFH-202b Questions Fee □ Latest CCFH-202b Version □ CCFH-202b Valid Exam Dumps □ Enter ▹ www.practicevce.com ◃ and search for □ CCFH-202b □ to download for free □CCFH-202b Accurate Answers
- CCFH-202b Paper □ CCFH-202b Valid Exam Pdf □ CCFH-202b Paper ☢ Search for ▸ CCFH-202b ◂ and download it for free immediately on ☀ www.pdfvce.com □☀□ □Latest CCFH-202b Version
- Reliable CrowdStrike CCFH-202b Practice Questions | Try Free Demo before Purchase □ Open website □ www.verifieddumps.com □ and search for ➡ CCFH-202b □□□ for free download ♥CCFH-202b Free Learning Cram
- CCFH-202b Valid Exam Pdf □ Valid CCFH-202b Practice Materials □ CCFH-202b Valid Exam Cost □ Search for 《 CCFH-202b 》 and obtain a free download on ➽ www.pdfvce.com □ □CCFH-202b New APP Simulations
- Valid CrowdStrike - CCFH-202b - CrowdStrike Certified Falcon Hunter Practice Questions □ Search for □ CCFH-202b □ and download it for free on ➽ www.prepawaypdf.com □ website □CCFH-202b Paper
- Free PDF 2026 CrowdStrike Latest CCFH-202b: CrowdStrike Certified Falcon Hunter Practice Questions ✌ Enter □ www.pdfvce.com □ and search for ➤ CCFH-202b □ to download for free ☣CCFH-202b Online Version
- CCFH-202b Paper □ CCFH-202b Valid Exam Pdf □ Latest CCFH-202b Exam Price □ Immediately open " www.troytecdumps.com " and search for ➤ CCFH-202b □ to obtain a free download □CCFH-202b Paper
- wzsj.lwtcc.cn, www.stes.tyc.edu.tw, pastebin.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, 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, 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, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that ActualTestsQuiz CCFH-202b dumps now are free: https://drive.google.com/open?id=1P5IM0uK5ZR_jRnrvcEKKK5cVqhDjGsUd