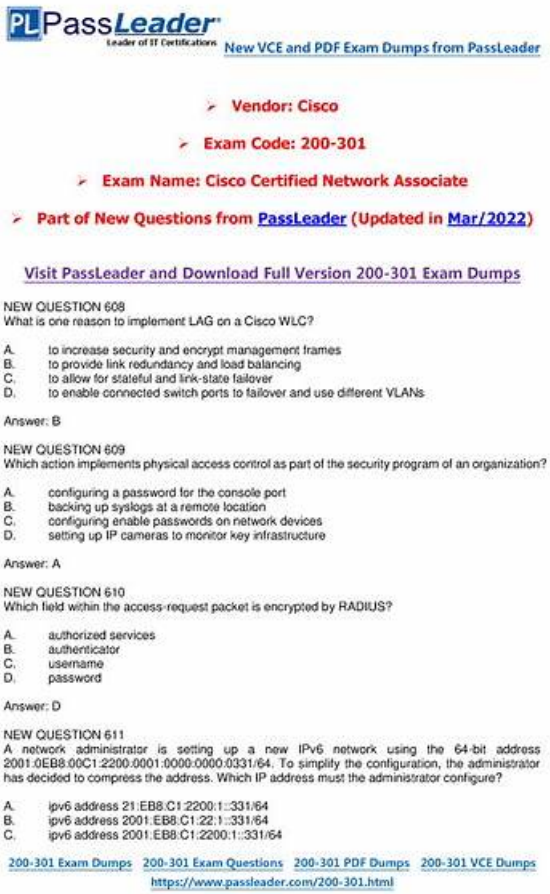
Pass Leader CCFH-202b Dumps - CCFH-202b Exam Preparation


PassLeader
Leader of IT Certifications
New VCE and PDF Exam Dumps from PassLeader

- Vendor: Cisco
- Exam Code: 200-301
- Exam Name: Cisco Certified Network Associate
- Part of New Questions from PassLeader (Updated in Mar/2022)

Visit PassLeader and Download Full Version 200-301 Exam Dumps

NEW QUESTION 608
What is one reason to implement LAG on a Cisco WLC?

A. to increase security and encrypt management frames
B. to provide link redundancy and load balancing
C. to allow for stateful and link-state failover
D. to enable connected switch ports to failover and use different VLANs

Answer: B

NEW QUESTION 609
Which action implements physical access control as part of the security program of an organization?

A. configuring a password for the console port
B. backing up syslogs at a remote location
C. configuring enable passwords on network devices
D. setting up IP cameras to monitor key infrastructure

Answer: A

NEW QUESTION 610
Which field within the access-request packet is encrypted by RADIUS?

A. authorized services
B. authenticator
C. username
D. password

Answer: D

NEW QUESTION 611
A network administrator is setting up a new IPv6 network using the 64-bit address 2001:0EB8:00C1:2200:0001:0000:0000:0331/64. To simplify the configuration, the administrator has decided to compress the address. Which IP address must the administrator configure?

A. ipv6 address 21:EB8:C1:2200:1::331/64
B. ipv6 address 2001:EB8:C1:22:1::331/64
C. ipv6 address 2001:EB8:C1:2200:1::331/64

200-301 Exam Dumps 200-301 Exam Questions 200-301 PDF Dumps 200-301 VCE Dumps
https://www.passleader.com/200-301.html

For candidates who are going to attend the exam, the pass rate is quite important. CCFH-202b training materials of us are pass guaranteed, and if you can't pass the exam one time, we are money back guaranteed. Besides CCFH-202b training materials are verified by skilled experts, therefore the quality and accuracy can be guaranteed, and you can use the CCFH-202b Exam Dumps at ease. We also have online and offline chat service stuff, if any other questions, please contact us, we will give a reply to you as quickly as possible.

CrowdStrike CCFH-202b Exam Syllabus Topics:

Topic	Details
Topic 1	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.
Topic 2	• 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 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	• 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	• Reports and References: This domain covers using built-in Hunt and Visibility reports and leveraging Events Full Reference documentation for event information.
Topic 6	• 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.

>> Pass Leader CCFH-202b Dumps <<

Free PDF Quiz CrowdStrike - Reliable Pass Leader CCFH-202b Dumps

We don't just want to make profitable deals, but also to help our users pass the CCFH-202b exams with the least amount of time to get a certificate. Choosing our CCFH-202b exam practice, you only need to spend 20-30 hours to prepare for the exam. Maybe you will ask whether such a short time can finish all the content, we want to tell you that you can rest assured ,because our CCFH-202b Learning Materials are closely related to the exam outline.

CrowdStrike Certified Falcon Hunter Sample Questions (Q20-Q25):

NEW QUESTION # 20
What do you click to jump to a Process Timeline from many pages in Falcon, such as a Hash Search?

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

Answer: B

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 # 21
Refer to Exhibit.
Falcon detected the above file attempting to execute. At initial glance; what indicators can we use to provide an initial analysis of the file?

- A. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled
- B. File path, hard disk volume number, and IOC Management action
- C. File name, path, Local and Global prevalence within the environment
- D. Local prevalence, IOC Management action, and Event Search

Answer: C

Explanation:
The file name, path, Local and Global prevalence are indicators that can provide an initial analysis of the file without relying on external sources or tools. The file name can indicate the purpose or origin of the file, such as if it is a legitimate application or a malicious payload. The file path can indicate where the file was located or executed from, such as if it was in a temporary or system directory. The Local and Global prevalence can indicate how common or rare the file is within the environment or across all Falcon customers, which can help assess the risk or impact of the file.

NEW QUESTION # 22

The help desk is reporting an increase in calls related to user accounts being locked out over the last few days. You suspect that this could be an attack by an adversary against your organization. Select the best hunting hypothesis from the following:

- A. Users are locking their accounts out because they recently changed their passwords
- B. A publicly available web application has been hacked and is causing the lockouts
- C. A password guessing attack is being executed against remote access mechanisms such as VPN
- D. A zero-day vulnerability is being exploited on a Microsoft Exchange server

Answer: C

Explanation:
A hunting hypothesis is a statement that describes a possible malicious activity that can be tested with data and analysis. A good hunting hypothesis should be specific, testable, and relevant to the problem or goal. In this case, the best hunting hypothesis from the following is that a password guessing attack is being executed against remote access mechanisms such as VPN, as it explains the possible cause and method of the user account lockouts in a specific and testable way. A zero-day vulnerability on a Microsoft Exchange server is too vague and does not explain how it relates to the lockouts. A hacked web application is also too vague and does not specify how it causes the lockouts. Users locking their accounts out because they recently changed their passwords is not a malicious activity and does not account for the increase in calls.

NEW QUESTION # 23
Which of the following queries will return the parent processes responsible for launching badprogram.exe?

- A. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename ParentProcessId_decimal AS TargetProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
- B. [search (ProcessList) where Name=badprogram.exe] | search ParentProcessName | table ParentProcessName _time
- C. event_simpleName=processrollup2 [search event_simpleName=processrollup2 FileName=badprogram.exe | rename TargetProcessId_decimal AS ParentProcessId_decimal | fields aid TargetProcessId_decimal] | stats count by FileName _time
- D. [search (ParentProcess) where name=badprogranrexe] | table ParentProcessName _time

Answer: C

Explanation:
This query will return the parent processes responsible for launching badprogram.exe by using a subsearch to find the processrollup2 events where FileName is badprogram.exe, then renaming the TargetProcessId_decimal field to ParentProcessId_decimal and using it as a filter for the main search, then using stats to count the occurrences of each FileName by _time. The other queries will either not return the parent processes or use incorrect field names or syntax.

NEW QUESTION # 24
Which threat framework allows a threat hunter to explore and model specific adversary tactics and techniques, with links to intelligence and case studies?

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

Answer: C

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 # 25
.....

As this version is called software version or PC version, maybe many candidates may think our CCFH-202b PC test engine may

just be used on personal computers. At first, it can be only used on PC. But with our IT staff's improvement, now our CrowdStrike CCFH-202b PC test engine can be installed on all electronic products. You can copy to your mobile, Ipad or others. No matter anywhere or any time you want to learn CCFH-202b PC test engine, it is convenient for you. For busy workers, you can make the best of your time on railway or bus, mastering one question and answers every time will be great.

CCFH-202b Exam Preparation: https://www.examcollectionpass.com/CrowdStrike/CCFH-202b-practice-exam-dumps.html

- Unparalleled Pass Leader CCFH-202b Dumps - Leader in Qualification Exams - Perfect CCFH-202b: CrowdStrike Certified Falcon Hunter □ Copy URL ⇛ www.vce4dumps.com ⇚ open and search for □ CCFH-202b □ to download for free □Exam CCFH-202b Book
- Premium CCFH-202b Exam ～ Reliable CCFH-202b Real Test □ Exam CCFH-202b Book □ Easily obtain free download of { CCFH-202b } by searching on ➤ www.pdfvce.com □ □CCFH-202b Reliable Study Questions
- CCFH-202b New Braindumps Pdf □ Exam CCFH-202b Book □ CCFH-202b Trustworthy Dumps ✔ Search for ✔ CCFH-202b □✔□ on ✔ www.dumpsquestion.com □✔□ immediately to obtain a free download □Hottest CCFH-202b Certification
- CCFH-202b Study Guide - CCFH-202b Test Dumps - CCFH-202b Practice Test □ Download ➽ CCFH-202b □ for free by simply searching on ➥ www.pdfvce.com □ ↪CCFH-202b Practice Test Online
- CCFH-202b Online Test □ CCFH-202b Valid Braindumps Questions □ Exam CCFH-202b Certification Cost □ Open ➠ www.practicevce.com □ enter ➽ CCFH-202b □ and obtain a free download □CCFH-202b Official Practice Test
- Seeing The Pass Leader CCFH-202b Dumps Means that You Have Passed Half of CrowdStrike Certified Falcon Hunter □ □ Search for ➥ CCFH-202b □ on ➠ www.pdfvce.com □ immediately to obtain a free download □CCFH-202b Official Practice Test
- Pass-Sure Pass Leader CCFH-202b Dumps – Find Shortcut to Pass CCFH-202b Exam □ Search for （ CCFH-202b ） and easily obtain a free download on ➡ www.dumpsmaterials.com □□□ □CCFH-202b Valid Braindumps Pdf
- Trustworthy CCFH-202b Exam Torrent □ CCFH-202b Practice Test Online □ CCFH-202b Practice Test Online □ Easily obtain ✔ CCFH-202b □✔□ for free download through 「 www.pdfvce.com 」 □CCFH-202b New Braindumps Pdf
- Pass-Sure Pass Leader CCFH-202b Dumps – Find Shortcut to Pass CCFH-202b Exam □ Search for ☀ CCFH-202b □☀□ on 「 www.prepawayete.com 」 immediately to obtain a free download □CCFH-202b Exam
- 2026 Pass Leader CCFH-202b Dumps | Valid CrowdStrike CCFH-202b Exam Preparation: CrowdStrike Certified Falcon Hunter □ Search for ➥ CCFH-202b □ and download it for free on □ www.pdfvce.com □ website □CCFH-202b Exams Collection
- CCFH-202b Valid Braindumps Pdf □ CCFH-202b New Braindumps Pdf □ Exam CCFH-202b Certification Cost □ Go to website 「 www.practicevce.com 」 open and search for [CCFH-202b] to download for free □Reliable CCFH-202b Real Test
- salamancaebookstore.com, www.stes.tyc.edu.tw, studio.eng.ku.ac.th, bbs.t-firefly.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, 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, Disposable vapes