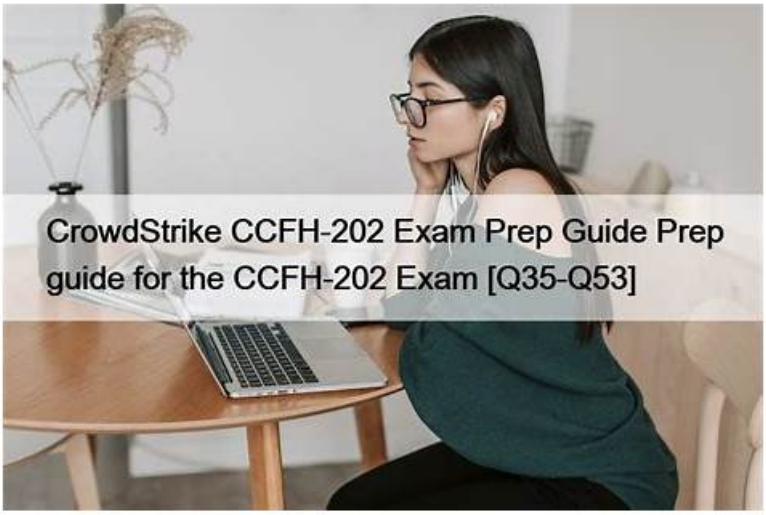
Reliable CCFH-202 Exam Camp & CCFH-202 Online Tests



P.S. Free & New CCFH-202 dumps are available on Google Drive shared by PDFBraindumps: https://drive.google.com/open?id=11Xq9gYJZmOzhT1qhdg-kzQrZQynBa85p

You must ensure that you can pass the CCFH-202 exam quickly, so you must choose an authoritative product. Our CCFH-202 exam materials are certified by the authority and have been tested by users. This is a product that you can definitely use with confidence. Of course, our data may make you more at ease. The passing rate of CCFH-202 Preparation prep reached 99%, which is a very incredible value, but we did. If you want to know more about our products, you can consult our staff, or you can download our free trial version of our CCFH-202 practice engine. We are looking forward to your joining.

CrowdStrike CCFH-202 Exam Syllabus Topics:

Topic	Details
Topic 1	• Explain what information is in the Hunting & Investigation Guide • Differentiate testing, DevOps or general user activity from adversary behavior
Topic 2	• Explain what information a Mac Sensor Report will provide • Conduct hypothesis and hunting lead generation to prove them out using Falcon tools
Topic 3	• Locate built-in Hunting reports and explain what they provide • Identify alternative analytical interpretations to minimize and reduce false positives
Topic 4	• Explain what information a Hash Execution Search provides • Explain what information a Bulk Domain Search provides
Topic 5	• Explain what information a Source IP Search provides • Explain what the “table” command does and demonstrate how it can be used for formatting output
Topic 6	• Identify the vulnerability exploited from an initial attack vector • Explain what information is in the Events Data Dictionary
Topic 7	• Convert and format Unix times to UTC-readable time • Evaluate information for reliability, validity and relevance for use in the process of elimination
Topic 8	• Demonstrate how to get a Process Timeline • Analyze and recognize suspicious overt malicious behaviors

>> Reliable CCFH-202 Exam Camp <<

CCFH-202 Online Tests | Knowledge CCFH-202 Points

You can imagine that you just need to pay a little money for our CCFH-202 exam prep, what you acquire is priceless. So it equals that you have made a worthwhile investment. Firstly, you will learn many useful knowledge and skills from our CCFH-202 Exam Guide, which is a valuable asset in your life. After all, no one can steal your knowledge. In addition, you can get the valuable CCFH-202 certificate.

CrowdStrike Certified Falcon Hunter Sample Questions (Q56-Q61):

NEW QUESTION # 56
An analyst has sorted all recent detections in the Falcon platform to identify the oldest in an effort to determine the possible first victim host What is this type of analysis called?

- A. Machine Learning
- B. Statistical analysis
- C. Visualization of hosts
- D. Temporal analysis

Answer: D

Explanation:
Temporal analysis is a type of analysis that focuses on the timing and sequence of events in order to identify patterns, trends, or anomalies. By sorting all recent detections in the Falcon platform to identify the oldest, an analyst can perform temporal analysis to determine the possible first victim host and trace back the origin of an attack.

NEW QUESTION # 57
In which of the following stages of the Cyber Kill Chain does the actor not interact with the victim endpoint(s)?

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

Answer: B

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 # 58
What is the difference between a Host Search and a Host Timeline?

- A. 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
- 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. 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

Answer: D

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 # 59
Which Falcon documentation guide should you reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts?

- A. Customizable Dashboards
- B. Events Data Dictionary
- C. Hunting and Investigation
- D. MITRE-Based Falcon Detections Framework

Answer: C

Explanation:
The Hunting and Investigation guide is the Falcon documentation guide that you should reference to hunt for anomalies related to scheduled tasks and other Windows related artifacts. The Hunting and Investigation guide provides sample hunting queries, select walkthroughs, and best practices for hunting with Falcon. It covers various topics such as process execution, network connections, registry activity, scheduled tasks, and more.

NEW QUESTION # 60
While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS " What does this User Name indicate?

- A. The User Name is not relevant for the dashboard
- B. The User Name is a System User
- C. There is no User Name associated with the event
- D. The Falcon sensor could not determine the User Name

Answer: C

Explanation:
When you see "hostnameS" in the User Name column in the Host Search page, it means that there is no User Name associated with the event. This can happen when the event is related to a system process or service that does not have a user context. It does not mean that the User Name is a System User, that the User Name is not relevant for the dashboard, or that the Falcon sensor could not determine the User Name.

NEW QUESTION # 61
.....

The most notable feature of the CCFH-202 learning quiz is that they provide you with the most practical solutions to help you learn the exam points of effortlessly and easily, then mastering the core information of the certification course outline. Their quality is much higher than the quality of any other materials, and questions and answers of CCFH-202 Training Materials contain information from the best available sources. Whether you are newbie or experienced exam candidates, our CCFH-202 study guide will relieve you of tremendous pressure and help you conquer the difficulties with efficiency.

Guide

- Valid CCFH-202 Exam Braindumps Supply You Trustable Practice Engine - www.prepawayete.com □ Go to website { www.prepawayete.com } open and search for 「 CCFH-202 」 to download for free □Valid CCFH-202 Braindumps
- Hot Reliable CCFH-202 Exam Camp | Efficient CrowdStrike CCFH-202 Online Tests: CrowdStrike Certified Falcon Hunter □ Download （ CCFH-202 ） for free by simply entering 「 www.pdfvce.com 」 website □New CCFH-202 Test Objectives
- Receive free updates for the CrowdStrike CCFH-202 Exam Dumps □ Download 《 CCFH-202 》 for free by simply entering ➤ www.validtorrent.com □ website □CCFH-202 Exams Torrent
- New Exam CCFH-202 Materials □ Reliable CCFH-202 Source □ New CCFH-202 Test Pattern □ Download 「 CCFH-202 」 for free by simply searching on ➡ www.pdfvce.com □□□ □New Exam CCFH-202 Materials
- Useful Reliable CCFH-202 Exam Camp - Passing CCFH-202 Exam is No More a Challenging Task □ Search for □ CCFH-202 □ on 「 www.vce4dumps.com 」 immediately to obtain a free download □CCFH-202 Pass4sure Dumps Pdf
- Test CCFH-202 Dump □ New CCFH-202 Test Pattern □ Exam CCFH-202 Revision Plan □ The page for free download of □ CCFH-202 □ on ✔ www.pdfvce.com □✔□ will open immediately □Latest CCFH-202 Real Test
- Useful Reliable CCFH-202 Exam Camp - Passing CCFH-202 Exam is No More a Challenging Task □ Open website ☀ www.easy4engine.com □☀□ and search for 《 CCFH-202 》 for free download □Latest CCFH-202 Real Test
- 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, wjhsd.instructure.com, bbs.t-firefly.com, 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, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New CCFH-202 dumps are available on Google Drive shared by PDFBraindumps: https://drive.google.com/open?id=11Xq9gYJZmOzhT1qhdg-kzQrZQynBa85p