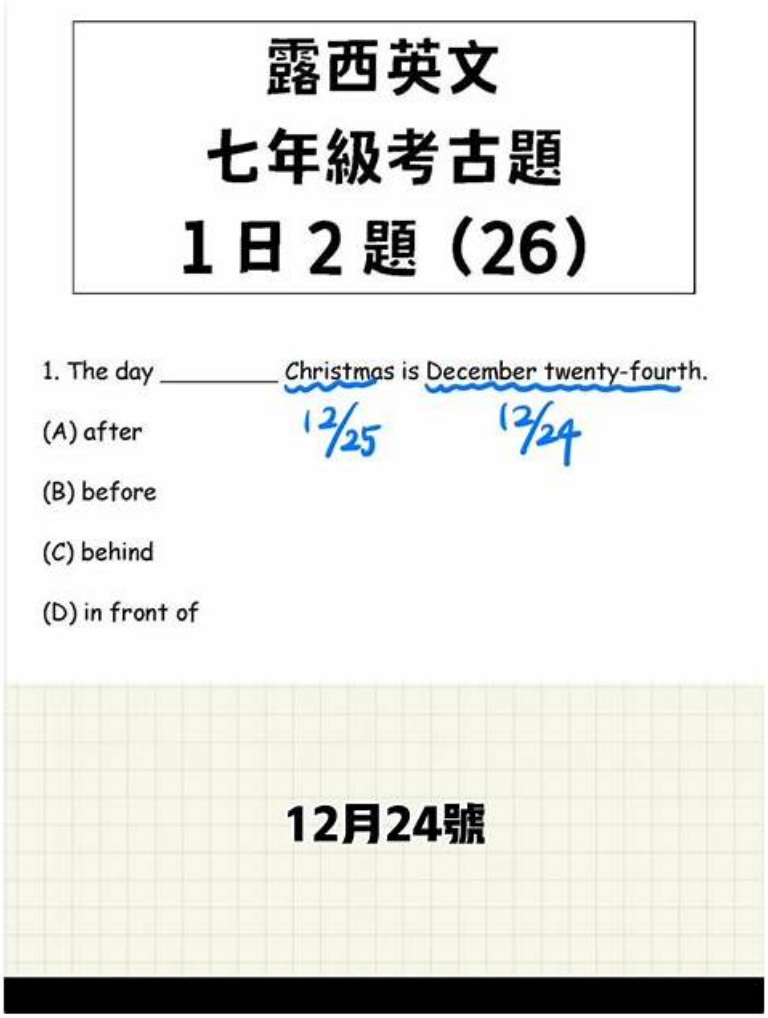
高質量的CCFH-202b考古題分享|高通過率的考試材料|確保通過的CCFH-202b：CrowdStrike Certified Falcon Hunter



P.S. VCESoft在Google Drive上分享了免費的、最新的CCFH-202b考試題庫：https://drive.google.com/open?id=16r-SaDxh-m8S4Fw9G3mfcbf8zJb7usqG

CCFH-202b資格認證考試是非常熱門的一項考試，雖然很難通過，但是你只要找准了切入點，考試合格並不是什麼難題。VCESoft就是你最好的選擇。VCESoft命中率高達100%的資料，可以幫你解決CCFH-202b考試上的任何難題，只要你認真學習資料上的問題，相信一切難題都可以迎刃而解，你購買了考古題以後還可以得到一年的免費更新服務，一年之內，只要你想更新你擁有的資料，那麼你就可以得到最新版。快點來體驗一下吧。

為通過CrowdStrike CCFH-202b 認證考試花大量的時間和精力復習相關知識，但是卻是冒險地通過考試。選擇VCESoft的產品卻可以讓你花少量的錢，一次性安全通過考試。我相信在如今時間如此寶貴的社會裏，VCESoft更適合你的選擇。而且我們的VCESoft是眾多類似網站中最能給你保障的一個網站，選擇VCESoft就等於選擇了成功。

>> CCFH-202b考古題分享 <<

CCFH-202b考試備考經驗，CCFH-202b最新題庫

VCESoft提供最新和準確的CrowdStrike CCFH-202b題庫資源，是考生通過考試和獲得證書最佳的方式。CCFH-202b認證是加快您作為IT行業專業人士的職業發展的最佳選擇。我們為幫助考生通過他們第一次嘗試的CCFH-202b考

試而感到自豪，在過去兩年里，CCFH-202b題庫的成功率絕對是令人驚嘆的，這是一個100%保證通過的學習資料。感謝我們的客戶，他們現在能夠在自己的職業生涯輝煌的發展，這些都歸功于VCESoft的考古題，值得信賴。

CrowdStrike CCFH-202b 考試大綱：

主題	簡介
主題 1	• Hunting Methodology: This domain covers conducting active hunts, performing outlier analysis, testing hunting hypotheses, constructing queries, and investigating process trees.
主題 2	• Detection Analysis: This domain focuses on analyzing Host and Process Timelines in Falcon to understand events and detections, and pivoting to additional investigative tools.
主題 3	• Search and Investigation Tools: This domain covers analyzing file and process metadata, using Investigate Module tools, performing various searches, and interpreting dashboard results.

最新的 CrowdStrike Falcon Certification Program CCFH-202b 免費考試真題 (Q39-Q44):

問題 #39
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. Choose the template you would like to configure, setup how often you would like the alert to run, and then schedule the alert
- D. Create the query for the alert, setup the email template for the alert, and then set the schedule for the alert

答案：B

解題說明：
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.

問題 #40
Which of the following is a suspicious process behavior?

- A. Non-network processes (eg, notepad exe) making an outbound network connection
- B. An Internet browser (eg, Internet Explorer) performing multiple DNS requests
- C. PowerShell running an execution policy of RemoteSigned
- D. PowerShell launching a PowerShell script

答案：A

解題說明：
Non-network processes are processes that are not expected to communicate over the network, such as notepad.exe. If they make an outbound network connection, it could indicate that they are compromised or maliciously used by an adversary. PowerShell running an execution policy of RemoteSigned is a default setting that allows local scripts to run without digital signatures. An Internet browser performing multiple DNS requests is a normal behavior for web browsing. PowerShell launching a PowerShell script is also a common behavior for legitimate tasks.

問題 #41

What information is provided when using IP Search to look up an IP address?

- A. Suspicious IP addresses
- B. Internal IPs only
- C. Both internal and external IPs
- D. External IPs only

答案：D

解題說明：
IP Search is an Investigate tool that allows you to look up information about external IPs only. It shows information such as geolocation, network connection events, detection history, etc. for each external IP address that has communicated with your hosts. It does not show information about internal IPs, suspicious IPs, or both internal and external IPs.

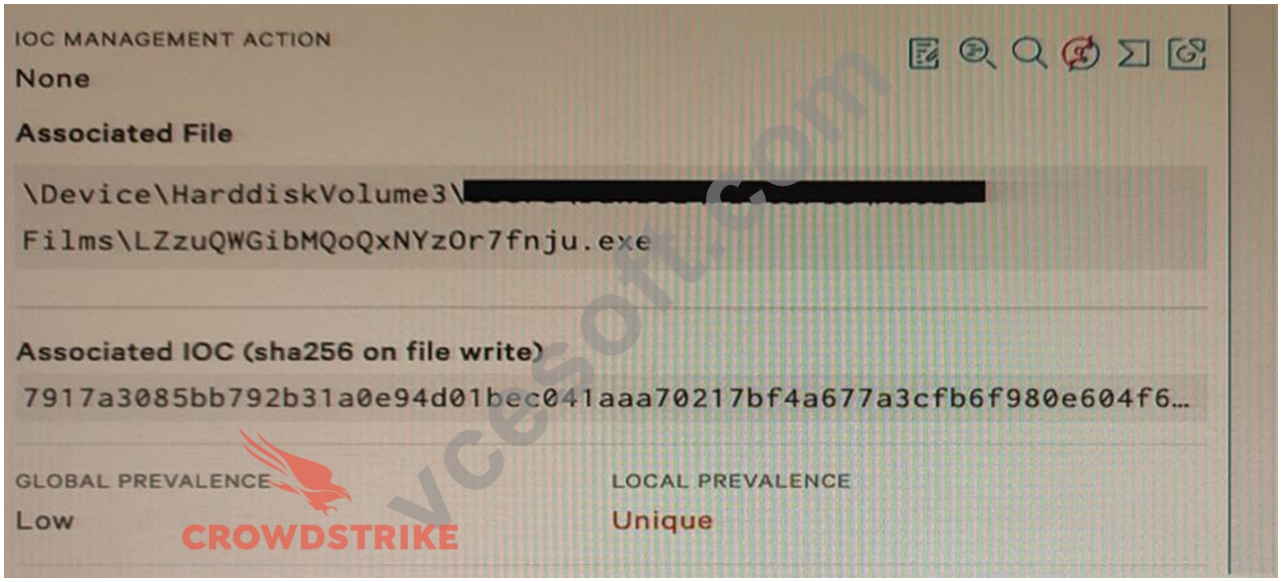
問題 #42
While you're reviewing Unresolved Detections in the Host Search page, you notice the User Name column contains "hostnameS " What does this User Name indicate?

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

答案：D

解題說明：
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.

問題 #43
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. File name, path, Local and Global prevalence within the environment
- B. VirusTotal, Hybrid Analysis, and Google pivot indicator lights enabled
- C. Local prevalence, IOC Management action, and Event Search
- D. File path, hard disk volume number, and IOC Management action

答案：A

解題說明：
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.

問題 #44
.....