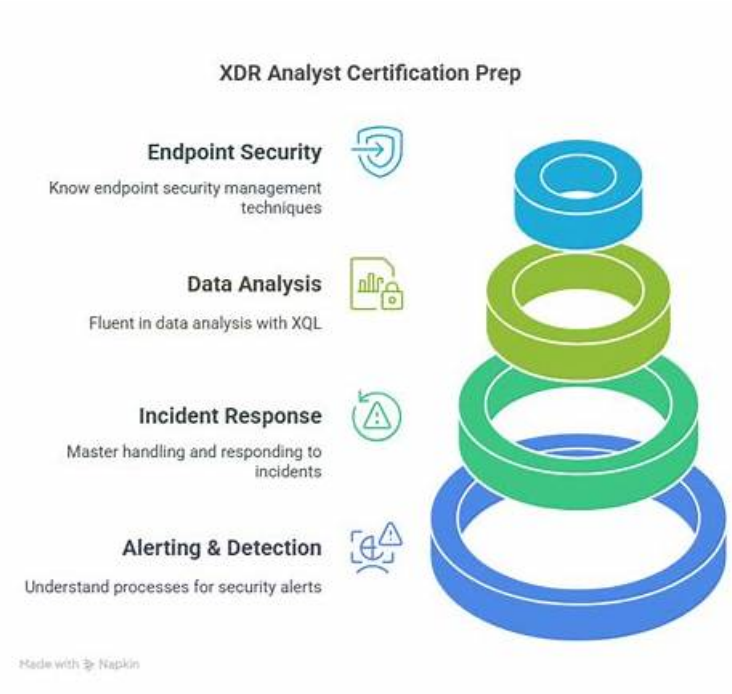
XDR-Analyst題庫更新，XDR-Analyst通過考試



如果你要購買我們的Palo Alto Networks的XDR-Analyst考題資料，VCESoft將提供最好的服務和最優質得的品質，我們的認證考試軟體已經取得了廠商和第三方的授權，並且擁有大量的IT業的專業及技術專家，根據客戶的需求，根據大綱開發出的一系列產品，以保證客戶的最大需求，Palo Alto Networks的XDR-Analyst考試認證資料具有最高的專業技術含量，可以作為相關知識的專家和學者學習和研究之用，我們提供所有的產品都有部分免費試用，在你購買之前以保證你考試的品質及適用性。

VCESoft為Palo Alto Networks XDR-Analyst 認證考試準備的培訓包括Palo Alto Networks XDR-Analyst認證考試的模擬測試題和當前的考試真題。在互聯網上你也可以看到幾個也提供相關的培訓的網站，但是你比較之後，你就會發現VCESoft的關於Palo Alto Networks XDR-Analyst 認證考試的培訓比較有針對性，不僅品質是最高的，而且內容是最全面的。

>> XDR-Analyst題庫更新 <<

高效的XDR-Analyst題庫更新和認證考試的領導者材料和權威的XDR-Analyst通過考試

你正在為了怎樣通過Palo Alto Networks的XDR-Analyst考試絞盡腦汁嗎？Palo Alto Networks的XDR-Analyst考試的認證資格是當代眾多IT認證考試中最有價值的資格之一。在近幾十年裏，IT已獲得了世界各地人們的關注，它已經成為了現代生活中不可或缺的一部分。其中，Palo Alto Networks的認證資格已經獲得了國際社會的廣泛認可。所以很多IT人士通過Palo Alto Networks的考試認證來提高自己的知識和技能。XDR-Analyst認證考試就是最重要的考試之一。這個認證資格能為大家帶來很大的好處。

Palo Alto Networks XDR-Analyst 考試大綱：

主題	簡介
主題 1	• Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights.

主題 2	• Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
主題 3	• Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions.
主題 4	• Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques.

最新的 Security Operations XDR-Analyst 免費考試真題 (Q79-Q84):

問題 #79
When creating a scheduled report which is not an option?

- A. Run weekly on a certain day and time.
- B. Run monthly on a certain day and time.
- C. Run quarterly on a certain day and time.
- D. Run daily at a certain time (selectable hours and minutes).

答案：C

解題說明：
When creating a scheduled report in Cortex XDR, the option to run quarterly on a certain day and time is not available. You can only schedule reports to run daily, weekly, or monthly. You can also specify the start and end dates, the time zone, and the recipients of the report. Scheduled reports are useful for generating regular reports on the security events, incidents, alerts, or endpoints in your network. You can create scheduled reports from the Reports page in the Cortex XDR console, or from the Query Center by saving a query as a report. Reference:
Run or Schedule Reports
Create a Scheduled Report

問題 #80
What kind of the threat typically encrypts user files?

- A. SQL injection attacks
- B. ransomware
- C. supply-chain attacks
- D. Zero-day exploits

答案：B

解題說明：
Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack123456 Reference:
What is Ransomware? | How to Protect Against Ransomware in 2023
Ransomware - Wikipedia
What is ransomware? | Ransomware meaning | Cloudflare
What Is Ransomware? | Ransomware.org
Ransomware - FBI

問題 #81
Which of the following is NOT a precanned script provided by Palo Alto Networks?

- A. list_directories
- B. process_kill_name
- C. quarantine_file
- D. delete_file

答案：A

解題說明：
Palo Alto Networks provides a set of precanned scripts that you can use to perform various actions on your endpoints, such as deleting files, killing processes, or quarantining malware. The precanned scripts are written in Python and are available in the Agent Script Library in the Cortex XDR console. You can use the precanned scripts as they are, or you can customize them to suit your needs. The precanned scripts are:
delete_file: Deletes a specific file from a local or removable drive.
quarantine_file: Moves a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
process_kill_name: Kills a process by its name on the endpoint.
process_kill_pid: Kills a process by its process ID (PID) on the endpoint.
process_kill_tree: Kills a process and all its child processes by its name on the endpoint.
process_kill_tree_pid: Kills a process and all its child processes by its PID on the endpoint.
process_list: Lists all the processes running on the endpoint, along with their names, PIDs, and command lines.
process_list_tree: Lists all the processes running on the endpoint, along with their names, PIDs, command lines, and parent processes.
process_start: Starts a process on the endpoint by its name or path.
registry_delete_key: Deletes a registry key and all its subkeys and values from the Windows registry.
registry_delete_value: Deletes a registry value from the Windows registry.
registry_list_key: Lists all the subkeys and values under a registry key in the Windows registry.
registry_list_value: Lists the value and data of a registry value in the Windows registry.
registry_set_value: Sets the value and data of a registry value in the Windows registry.
The script list_directories is not a precanned script provided by Palo Alto Networks. It is a custom script that you can write yourself using Python commands.
Reference:
Run Scripts on an Endpoint
Agent Script Library
Precanned Scripts

問題 #82
Which version of python is used in live terminal?

- A. Python 2 and 3 with specific XDR Python libraries developed by Palo Alto Networks
- B. Python 3 with standard Python libraries
- C. Python 2 and 3 with standard Python libraries
- D. Python 3 with specific XDR Python libraries developed by Palo Alto Networks

答案：B

解題說明：
Live terminal uses Python 3 with standard Python libraries to run Python commands and scripts on the endpoint. Live terminal does not support Python 2 or any custom or external Python libraries. Live terminal uses the Python interpreter embedded in the Cortex XDR agent, which is based on Python 3.7.4. The standard Python libraries are the modules that are included with the Python installation and provide a wide range of functionalities, such as operating system interfaces, network programming, data processing, and more. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint, such as querying system information, modifying files or registry keys, or running other applications. Reference:
Run Python Commands and Scripts
Python Standard Library

問題 #83
When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

- A. Investigate several Incidents at once.
- B. Assign incidents to an analyst in bulk.
- C. Change the status of multiple incidents.
- D. Delete the selected Incidents.

答案：B,C

解題說明：
When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents12 Reference:
Assign Incidents to an Analyst in Bulk
Change the Status of Multiple Incidents

問題 #84
.....

www.stes.tyc.edu.tw, www.lilly-angel.co.uk, 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, academy.frenchrealm.com, www.stes.tyc.edu.tw, Disposable vapes