XDR-Analyst Valid Braindumps Files - New XDR-Analyst Dumps Ebook

Achieving the Palo Alto Networks XDR-Analyst certificate is an excellent way of paying your way in the tech field. However, to become Palo Alto Networks XDR-Analyst certified, you will have to crack the Palo Alto Networks XDR-Analyst exam. This is a challenging task since preparation for the Palo Alto Networks XDR-Analyst Exam demands an inside-out understanding of XDR-Analyst domains and many Palo Alto Networks XDR-Analyst test applicants do not have enough time due to their busy routines.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
Topic 3	• 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.
Topic 4	• 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.

>> XDR-Analyst Valid Braindumps Files <<

Quiz XDR-Analyst - Trustable Palo Alto Networks XDR Analyst Valid

Braindumps Files

It is similar to the XDR-Analyst desktop-based software, with all the elements of the desktop practice exam. This mock exam can be accessed from any browser and does not require installation. The Palo Alto Networks XDR Analyst (XDR-Analyst) questions in the mock test are the same as those in the real exam. And candidates will be able to take the web-based Palo Alto Networks XDR Analyst (XDR-Analyst) practice test immediately through any operating system and browsers.

Palo Alto Networks XDR Analyst Sample Questions (Q77-Q82):

NEW QUESTION # 77
Which type of IOC can you define in Cortex XDR?

- A. Destination IP Address
- B. Source IP Address
- C. Source port
- D. Destination IP Address: Destination

Answer: A

Explanation:
Cortex XDR allows you to define IOC rules based on various types of indicators of compromise (IOC) that you can use to detect and respond to threats in your network. One of the types of IOC that you can define in Cortex XDR is destination IP address, which is the IP address of the remote host that a local endpoint is communicating with. You can use this type of IOC to identify malicious network activity, such as connections to command and control servers, phishing sites, or malware distribution hosts. You can also specify the direction of the network traffic (inbound or outbound) and the protocol (TCP or UDP) for the destination IP address IOC. Reference:
Cortex XDR documentation portal
Is there a possibility to create an IOC list to employ it in a query?
Cortex XDR Datasheet

NEW QUESTION # 78
Which of the following is NOT a precanned script provided by Palo Alto Networks?

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

Answer: B

Explanation:
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

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

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

Answer: D

Explanation:
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

NEW QUESTION # 80
When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. Unassigned
- B. Pending
- C. New
- D. It is blank

Answer: A

Explanation:
The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
B . It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group12.
D . New: This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"3.
In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.
Reference:
Cortex XDR Pro Admin Guide: Manage Incidents
Cortex XDR Pro Admin Guide: Assign Incidents
Cortex XDR Pro Admin Guide: Update Incident Status

NEW QUESTION # 81
Phishing belongs to which of the following MITRE ATT&CK tactics?

- A. Persistence, Command and Control
- B. Reconnaissance, Persistence
- C. Initial Access, Persistence
- D. Reconnaissance, Initial Access

Answer: D

Explanation:
Phishing is a technique that belongs to two MITRE ATT&CK tactics: Reconnaissance and Initial Access. Reconnaissance is the process of gathering information about a target before launching an attack. Phishing for information is a sub-technique of Reconnaissance that involves sending phishing messages to elicit sensitive information that can be used during targeting. Initial Access is the process of gaining a foothold in a network or system. Phishing is a sub-technique of Initial Access that involves sending phishing messages to execute malicious code on victim systems. Phishing can be used for both Reconnaissance and Initial Access depending on the objective and content of the phishing message. Reference:
Phishing, Technique T1566 - Enterprise | MITRE ATT&CK 1
Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK 2 Phishing for information, Part 2: Tactics and techniques 3 PHISHING AND THE MITREATT&CK FRAMEWORK - EnterpriseTalk 4 Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK 5

NEW QUESTION # 82
.....

Having more competitive advantage means that you will have more opportunities and have a job that will satisfy you. This is why more and more people have long been eager for the certification of XDR-Analyst. Our XDR-Analyst test material can help you focus and learn effectively. You don't have to worry about not having a dedicated time to learn every day. You can learn our XDR-Analyst exam torrent in a piecemeal time, and you don't have to worry about the tedious and cumbersome learning content. We will simplify the complex concepts by adding diagrams and examples during your study. By choosing our XDR-Analyst test material, you will be able to use time more effectively than others and have the content of important information in the shortest time.

for 「 XDR-Analyst 」 on 「 www.pdfdumps.com 」 immediately to obtain a free download □New XDR-Analyst Test Vce Free

- 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, lovecassie.ca, 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, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, kapoorclasses.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, myportal.utt.edu.tt, Disposable vapes