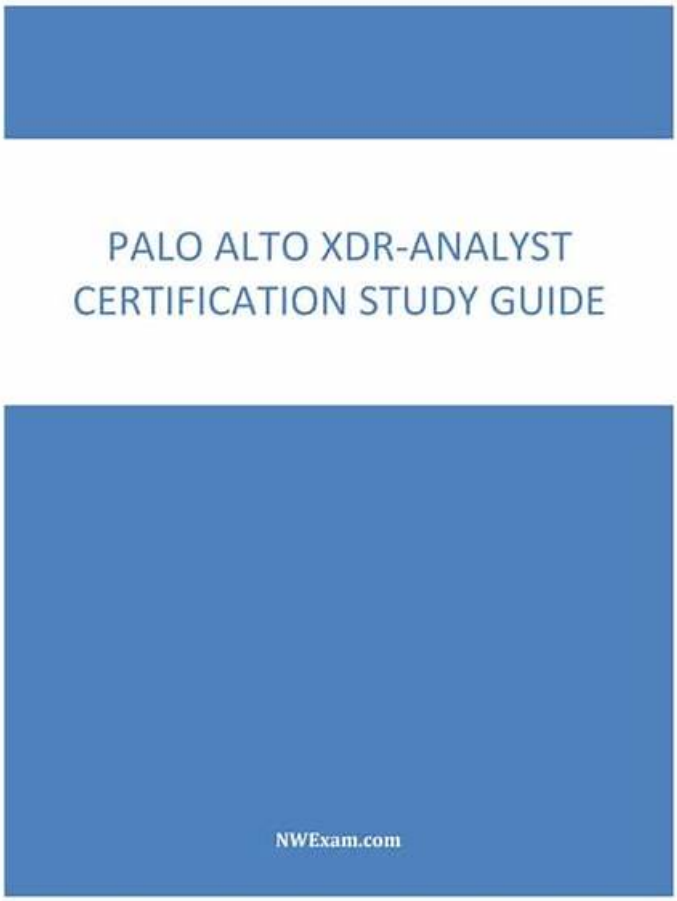
Pass Guaranteed XDR-Analyst - Palo Alto Networks XDR Analyst Accurate Valid Dumps Pdf



There is nothing more exciting than an effective and useful XDR-Analyst question bank if you want to get the XDR-Analyst certification in the least time by the first attempt. The sooner you use our XDR-Analysttraining materials, the more chance you will pass XDR-Analyst the exam, and the earlier you get your XDR-Analyst certificate. You definitely have to have a try on our XDR-Analyst exam questions and you will be satisfied without doubt. Besides that, We are amply praised by our customers all over the world not only for our valid and accurate XDR-Analyst study materials, but also for our excellent service.

The company is preparing for the test candidates to prepare the XDR-Analyst exam guide professional brand, designed to be the most effective and easiest way to help users through their want to get the test XDR-Analyst certification and obtain the relevant certification. In comparison with similar educational products, our training materials are of superior quality and reasonable price, so our company has become the top enterprise in the international market. Our XDR-Analyst practice materials have been well received by the users, mainly reflected in the following advantages.

>> Valid Dumps XDR-Analyst Pdf <<

XDR-Analyst New Braindumps Files - XDR-Analyst Latest Exam Review

Our XDR-Analyst study guide provide you with three different versions including PC、App and PDF version. Each version has the same questions and answers, and you can choose one from them or three packaged downloads of XDR-Analyst training materials. In addition to a wide variety of versions, our learning materials can be downloaded and used immediately after payment. We believe you will understand the convenience and power of our XDR-Analyst Study Guide through the pre-purchase trial.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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.
Topic 4	• 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.

Palo Alto Networks XDR Analyst Sample Questions (Q83-Q88):

NEW QUESTION # 83
Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

- A. exception profiles that apply to specific endpoints
- B. global exception profiles that apply to all endpoints
- C. agent exception profiles that apply to specific endpoints
- D. role-based profiles that apply to specific endpoints

Answer: B,C

Explanation:
Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. Reference:
Exception Security Profiles
Create an Agent Exception Profile
Create a Global Exception Profile

NEW QUESTION # 84
What is the outcome of creating and implementing an alert exclusion?

- A. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.
- B. The Cortex XDR console will hide those alerts.
- C. The Cortex XDR agent will not create an alert for this event in the future.
- D. The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Answer: B

Explanation:
The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create

an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint. Therefore, the correct answer is B, the Cortex XDR console will hide those alerts12 Reference:
Alert Exclusions
Create an Alert Exclusion Policy

NEW QUESTION # 85
If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

- A. Local Agent Installer and Content Caching
- B. Local Agent Proxy
- C. Broker VM Pathfinder
- D. Broker VM Syslog Collector

Answer: B

Explanation:
If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it here1 and here2. Reference:
Local Agent Proxy
Configure the Local Agent Proxy Setup

NEW QUESTION # 86
Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

- A. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.
- B. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.
- C. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.
- D. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.

Answer: A

Explanation:
To add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint, you need to use the Action Center in Cortex XDR. The Action Center allows you to create and manage actions that apply to endpoints, such as adding files or processes to the allow list or block list, isolating or unisolating endpoints, or initiating live terminal sessions. To add a file hash to the allow list, you need to choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it. This will prevent the Malware profile from scanning or blocking the file on the endpoints that match the scope of the action. Reference: Cortex XDR 3: Responding to Attacks1, Action Center2

NEW QUESTION # 87
Which Exploit Protection Module (EPM) can be used to prevent attacks based on OS function?

- A. DLL Security

- B. UASLR
- C. Memory Limit Heap Spray Check
- D. JIT Mitigation

Answer: D

Explanation:
JIT Mitigation is an Exploit Protection Module (EPM) that can be used to prevent attacks based on OS function. JIT Mitigation protects against exploits that use the Just-In-Time (JIT) compiler of the OS to execute malicious code. JIT Mitigation monitors the memory pages that are allocated by the JIT compiler and blocks any attempts to execute code from those pages. This prevents attackers from using the JIT compiler as a way to bypass other security mechanisms such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Reference:
Palo Alto Networks. (2023). PCDRA Study Guide. PDF file. Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf Palo Alto Networks. (2021). Exploit Protection Modules. Web page. Retrieved from https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-security-policies/exploit-protection-modules.html

NEW QUESTION # 88
.....

Therefore, you have the option to use Palo Alto Networks XDR-Analyst PDF questions anywhere and anytime. XDR-Analyst dumps are designed according to the Palo Alto Networks XDR Analyst (XDR-Analyst) certification exam standard and have hundreds of questions similar to the actual XDR-Analyst Exam. BraindumpQuiz Palo Alto Networks XDR Analyst (XDR-Analyst) web-based practice exam software also works without installation.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, wzsj.lwtcc.cn, ncon.edu.sa, www.4shared.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.sxrsedu.cn, Disposable vapes