

Dumps XDR-Engineer PDF - Exam XDR-Engineer Prep

Download Valid XDR Engineer Exam Dumps For Best Preparation

Exam : **XDR Engineer**

Title : Palo Alto Networks XDR
Engineer

<https://www.passcert.com/XDR-Engineer.html>

1 / 4

P.S. Free 2026 Palo Alto Networks XDR-Engineer dumps are available on Google Drive shared by Exams4Collection:
https://drive.google.com/open?id=159dwFIBkkteLEw5sU_SP2u3Q5vx16uVK

There may be customers who are concerned about the installation or use of our XDR-Engineer training questions. You don't have to worry about this. In addition to high quality and high efficiency, considerate service is also a big advantage of our company. We will provide 24 - hour online after-sales service to every customer. If you have any questions about installing or using our XDR-Engineer Real Exam, our professional after-sales service staff will provide you with warm remote service. As long as it is about our XDR-Engineer learning materials, we will be able to solve. Whether you're emailing or contacting us online, we'll help you solve the problem as quickly as possible. You don't need any worries at all.

Nowadays in this information-based world the definition of the talents has changed a lot and the talents mean that the personnel boost both the knowledge in XDR-Engineer area and the practical abilities now. So if you want to be the talent the society actually needs you must apply your knowledge into the practical working and passing the test XDR-Engineer Certification can make you become the talent the society needs. If you buy our XDR-Engineer study materials you will pass the XDR-Engineer exam successfully and realize your goal to be the talent.

>> Dumps XDR-Engineer PDF <<

Free PDF Dumps XDR-Engineer PDF - Pass XDR-Engineer in One Time - High-quality Exam XDR-Engineer Prep

The content of our XDR-Engineer quiz torrent is imbued with useful exam questions easily appear in the real condition. We are still moderately developing our latest XDR-Engineer exam torrent all the time to help you cope with difficulties. All exam candidates

make overt progress after using our XDR-Engineer Quiz torrent. By devoting ourselves to providing high-quality practice materials to our customers all these years, we can guarantee all content are the essential part to practice and remember. Stop dithering and make up your mind at once, XDR-Engineer test prep will not let you down.

Palo Alto Networks XDR Engineer Sample Questions (Q49-Q54):

NEW QUESTION # 49

How are dynamic endpoint groups created and managed in Cortex XDR?

- A. Endpoint groups require intervention to update the group with new endpoints when a new device is added to the network
- B. Each endpoint can belong to multiple groups simultaneously, allowing different security policies to be applied to the same device at the same time
- C. After an endpoint group is created, its assigned security policy cannot be changed without deleting and recreating the group
- **D. Endpoint groups are defined based on fields such as OS type, OS version, and network segment**

Answer: D

Explanation:

In Cortex XDR, dynamic endpoint groups are used to organize endpoints for applying security policies, managing configurations, and streamlining operations. These groups are defined based on dynamic criteria, such as OS type, OS version, network segment, hostname, or other endpoint attributes. When a new endpoint is added to the network, it is automatically assigned to the appropriate group(s) based on these criteria, without manual intervention. This dynamic assignment ensures that security policies are consistently applied to endpoints matching the group's conditions.

* Correct Answer Analysis (D): The option D accurately describes how dynamic endpoint groups are created and managed. Administrators define groups using filters based on endpoint attributes like operating system (e.g., Windows, macOS, Linux), OS version (e.g., Windows 10 21H2), or network segment (e.g., subnet or domain). These filters are evaluated dynamically, so endpoints are automatically added or removed from groups as their attributes change or new devices are onboarded.

* Why not the other options?

* A. Endpoint groups require intervention to update the group with new endpoints when a new device is added to the network: This is incorrect because dynamic endpoint groups are designed to automatically include new endpoints that match the group's criteria, without manual intervention.

* B. Each endpoint can belong to multiple groups simultaneously, allowing different security policies to be applied to the same device at the same time: This is incorrect because, in Cortex XDR, an endpoint is assigned to a single endpoint group for policy application to avoid conflicts.

While endpoints can match multiple group criteria, the system uses a priority or hierarchy to assign the endpoint to one group for policy enforcement.

* C. After an endpoint group is created, its assigned security policy cannot be changed without deleting and recreating the group: This is incorrect because Cortex XDR allows administrators to modify the security policy assigned to an endpoint group without deleting and recreating the group.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains endpoint group management: "Dynamic endpoint groups are created by defining filters based on endpoint attributes such as OS type, version, or network segment.

Endpoints are automatically assigned to groups based on these criteria" (paraphrased from the Endpoint Management section).

The EDU-260: Cortex XDR Prevention and Deployment course covers endpoint group configuration, stating that "groups are dynamically updated as endpoints join or leave the network based on defined attributes" (paraphrased from course materials).

The Palo Alto Networks Certified XDR Engineer datasheet includes "endpoint management and policy configuration" as a key exam topic, which encompasses dynamic endpoint groups.

References:

Palo Alto Networks Cortex XDR Documentation Portal: <https://docs-cortex.paloaltonetworks.com/> EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer

Datasheet: <https://www.paloaltonetworks.com/services/education/certification/#xdr-engineer>

NEW QUESTION # 50

When using Kerberos as the authentication method for Pathfinder, which two settings must be validated on the DNS server? (Choose two.)

- A. AD DS-integrated zones
- **B. Reverse DNS records**

- C. DNS forwarders
- **D. Reverse DNS zone**

Answer: B,D

Explanation:

Pathfinder in Cortex XDR is a tool for discovering unmanaged endpoints in a network, often using authentication methods like Kerberos to access systems securely. Kerberos authentication relies heavily on DNS for resolving hostnames and ensuring proper communication between clients, servers, and the Kerberos Key Distribution Center (KDC). Specific DNS settings must be validated to ensure Kerberos authentication works correctly for Pathfinder.

* Correct Answer Analysis (B, C):

* B. Reverse DNS zone: A reverse DNS zone is required to map IP addresses to hostnames (PTR records), which Kerberos uses to verify the identity of servers and clients. Without a properly configured reverse DNS zone, Kerberos authentication may fail due to hostname resolution issues.

* C. Reverse DNS records: Reverse DNS records (PTR records) within the reverse DNS zone must be correctly configured for all relevant hosts. These records ensure that IP addresses resolve to the correct hostnames, which is critical for Kerberos to authenticate Pathfinder's access to endpoints.

* Why not the other options?

* A. DNS forwarders: DNS forwarders are used to route DNS queries to external servers when a local DNS server cannot resolve them. While useful for general DNS resolution, they are not specifically required for Kerberos authentication or Pathfinder.

* D. AD DS-integrated zones: Active Directory Domain Services (AD DS)-integrated zones enhance DNS management in AD environments, but they are not strictly required for Kerberos authentication. Kerberos relies on proper forward and reverse DNS resolution, not AD-specific DNS configurations.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains Pathfinder configuration: "For Kerberos authentication, ensure that the DNS server has a properly configured reverse DNS zone and reverse DNS records to support hostname resolution" (paraphrased from the Pathfinder Configuration section). The EDU-260: Cortex XDR Prevention and Deployment course covers Pathfinder setup, stating that "Kerberos requires valid reverse DNS zones and PTR records for authentication" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes "planning and installation" as a key exam topic, encompassing Pathfinder authentication settings.

References:

Palo Alto Networks Cortex XDR Documentation Portal: <https://docs-cortex.paloaltonetworks.com/> EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet: <https://www.paloaltonetworks.com/services/education/certification/#xdr-engineer>

NEW QUESTION # 51

In addition to using valid authentication credentials, what is required to enable the setup of the Database Collector applet on the Broker VM to ingest database activity?

- A. Access to the database audit log
- **B. Valid SQL query targeting the desired data**
- C. Database schema exported in the correct format
- D. Access to the database transaction log

Answer: B

Explanation:

The Database Collector applet on the Broker VM in Cortex XDR is used to ingest database activity logs by querying the database directly. To set up the applet, valid authentication credentials (e.g., username and password) are required to connect to the database. Additionally, a valid SQL query must be provided to specify the data to be collected, such as specific tables, columns, or events (e.g., login activity or data modifications).

* Correct Answer Analysis (A): A valid SQL query targeting the desired data is required to configure the Database Collector applet. The query defines which database records or events are retrieved and sent to Cortex XDR for analysis. This ensures the applet collects only the relevant data, optimizing ingestion and analysis.

* Why not the other options?

* B. Access to the database audit log: While audit logs may contain relevant activity, the Database Collector applet queries the database directly using SQL, not by accessing audit logs.

Audit logs are typically ingested via other methods, such as Filebeat or syslog.

* C. Database schema exported in the correct format: The Database Collector does not require an exported schema. The SQL

query defines the data structure implicitly, and Cortex XDR maps the queried data to its schema during ingestion.

* D. Access to the database transaction log: Transaction logs are used for database recovery or replication, not for direct data collection by the Database Collector applet, which relies on SQL queries.

Exact Extract or Reference:

The Cortex XDR Documentation Portal describes the Database Collector applet: "To configure the Database Collector, provide valid authentication credentials and a valid SQL query to retrieve the desired database activity" (paraphrased from the Broker VM Applets section). The EDU-260: Cortex XDR Prevention and Deployment course covers data ingestion, stating that "the Database Collector applet requires a SQL query to specify the data to ingest from the database" (paraphrased from course materials).

The Palo Alto Networks Certified XDR Engineer datasheet includes "data ingestion and integration" as a key exam topic, encompassing Database Collector configuration.

References:

Palo Alto Networks Cortex XDR Documentation Portal: <https://docs-cortex.paloaltonetworks.com/> EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer

Datasheet: <https://www.paloaltonetworks.com/services/education/certification#xdr-engineer>

NEW QUESTION # 52

What happens when the XDR Collector is uninstalled from an endpoint by using the Cortex XDR console?

- A. It is uninstalled during the next heartbeat communication, machine status changes to Uninstalled, and the configuration data is retained for 90 days
- B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days
- C. The files are removed immediately, and the machine is deleted from the system without any retention period
- D. The associated configuration data is removed from the Action Center immediately after uninstallation

Answer: A

Explanation:

The XDR Collector is a lightweight agent in Cortex XDR used to collect logs and events from endpoints or servers. When uninstalled via the Cortex XDR console, the uninstallation process is initiated remotely, but the actual removal occurs during the endpoint's next communication with the Cortex XDR tenant, known as the heartbeat. The heartbeat interval is typically every few minutes, ensuring timely uninstallation. After uninstallation, the machine's status in the console updates, and associated configuration data is retained for a specific period to support potential reinstallation or auditing.

* Correct Answer Analysis (C): When the XDR Collector is uninstalled using the Cortex XDR console, it is uninstalled during the next heartbeat communication, the machine status changes to Uninstalled, and the configuration data is retained for 90 days. This retention period allows administrators to review historical data or reinstall the collector if needed, after which the data is permanently deleted.

* Why not the other options?

* A. The files are removed immediately, and the machine is deleted from the system without any retention period: Uninstallation is not immediate; it occurs at the next heartbeat.

Additionally, Cortex XDR retains configuration data for a period, not deleting it immediately.

* B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days: The machine status updates to Uninstalled automatically, not requiring manual removal, and the retention period is 90 days, not seven days.

* D. The associated configuration data is removed from the Action Center immediately after uninstallation: Configuration data is retained for 90 days, not removed immediately, and the Action Center is not the primary location for this data.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains XDR Collector uninstallation: "When uninstalled via the console, the XDR Collector is removed at the next heartbeat, the machine status changes to Uninstalled, and configuration data is retained for 90 days" (paraphrased from the XDR Collector Management section). The EDU-260: Cortex XDR Prevention and Deployment course covers collector management, stating that

"uninstallation occurs at the next heartbeat, with a 90-day retention period for configuration data" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes

"post-deployment management and configuration" as a key exam topic, encompassing XDR Collector uninstallation.

References:

Palo Alto Networks Cortex XDR Documentation Portal: <https://docs-cortex.paloaltonetworks.com/> EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer

Datasheet: <https://www.paloaltonetworks.com/services/education/certification#xdr-engineer>

NEW QUESTION # 53

How can a Malware profile be configured to prevent a specific executable from being uploaded to the cloud?

- A. Disable on-demand file examination for the executable
- B. Add the executable to the allow list for executions
- **C. Create an exclusion rule for the executable**
- D. Set PE and DLL examination for the executable to report action mode

Answer: C

Explanation:

In Cortex XDR, Malware profiles define how the agent handles files for analysis, including whether they are uploaded to the cloud for WildFire analysis or other cloud-based inspections. To prevent a specific executable from being uploaded to the cloud, the administrator can configure an exclusion rule in the Malware profile.

Exclusion rules allow specific files, directories, or patterns to be excluded from cloud analysis, ensuring they are not sent to the cloud while still allowing local analysis or other policy enforcement.

* Correct Answer Analysis (D): Creating an exclusion rule for the executable in the Malware profile ensures that the specified file is not uploaded to the cloud for analysis. This can be done by specifying the file's name, hash, or path in the exclusion settings, preventing unnecessary cloud uploads while maintaining agent functionality for other files.

* Why not the other options?

* A. Disable on-demand file examination for the executable: Disabling on-demand file examination prevents the agent from analyzing the file at all, which could compromise security by bypassing local and cloud analysis entirely. This is not the intended solution.

* B. Set PE and DLL examination for the executable to report action mode: Setting examination to "report action mode" configures the agent to log actions without blocking or uploading, but it does not specifically prevent cloud uploads. This option is unrelated to controlling cloud analysis.

* C. Add the executable to the allow list for executions: Adding an executable to the allow list permits it to run without triggering prevention actions, but it does not prevent the file from being uploaded to the cloud for analysis.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains Malware profile configuration: "Exclusion rules in Malware profiles allow administrators to specify files or directories that are excluded from cloud analysis, preventing uploads to WildFire or other cloud services" (paraphrased from the Malware Profile Configuration section). The EDU-260: Cortex XDR Prevention and Deployment course covers agent configuration, stating that "exclusion rules can be used to prevent specific files from being sent to the cloud for analysis" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes "Cortex XDR agent configuration" as a key exam topic, encompassing Malware profile settings.

References:

Palo Alto Networks Cortex XDR Documentation Portal: <https://docs-cortex.paloaltonetworks.com/> EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet: <https://www.paloaltonetworks.com/services/education/certification#xdr-engineer>

NEW QUESTION # 54

.....

Many people want to be the competent people which can excel in the job in some area and be skillful in applying the knowledge to the practical working in some industry. But the thing is not so easy for them they need many efforts to achieve their goals. Passing the XDR-Engineer test certification can make them become that kind of people and if you are one of them buying our XDR-Engineer study materials will help you pass the XDR-Engineer test smoothly with few efforts needed.

Exam XDR-Engineer Prep: <https://www.exams4collection.com/XDR-Engineer-latest-braindumps.html>

If you encounter similar questions during the installation of the XDR-Engineer practice questions, our staffs will provide you with remote technical guidance, Palo Alto Networks Dumps XDR-Engineer PDF And the long-term researches about actual questions of past years are the essential part to practice and remember, Palo Alto Networks Dumps XDR-Engineer PDF Keeping hard working and constantly self-enhancement make you grow up fast and gain a lot of precious opportunities.

Today's business leaders are confronted with a variety of obstacles that threaten their very survival, You have right to try out the XDR-Engineer demo freely on our product page and make clear what version is suitable.

If you encounter similar questions during the installation of the XDR-Engineer Practice Questions, our staffs will provide you with remote technical guidance, And the long-term researches XDR-Engineer Braindump Free about actual questions of past years are the essential part to practice and remember.

Our XDR-Engineer test braindump materials is popular based on that too.

- BONUS!!! Download part of Exams4Collection XDR-Engineer dumps for free: https://drive.google.com/open?id=159dwFIBkkteLEw5sU_SP2u3Q5vx16uVK

BONUS!!! Download part of Exams4Collection XDR-Engineer dumps for free: https://drive.google.com/open?id=159dwFIBkkteLEw5sU_SP2u3Q5vx16uVK