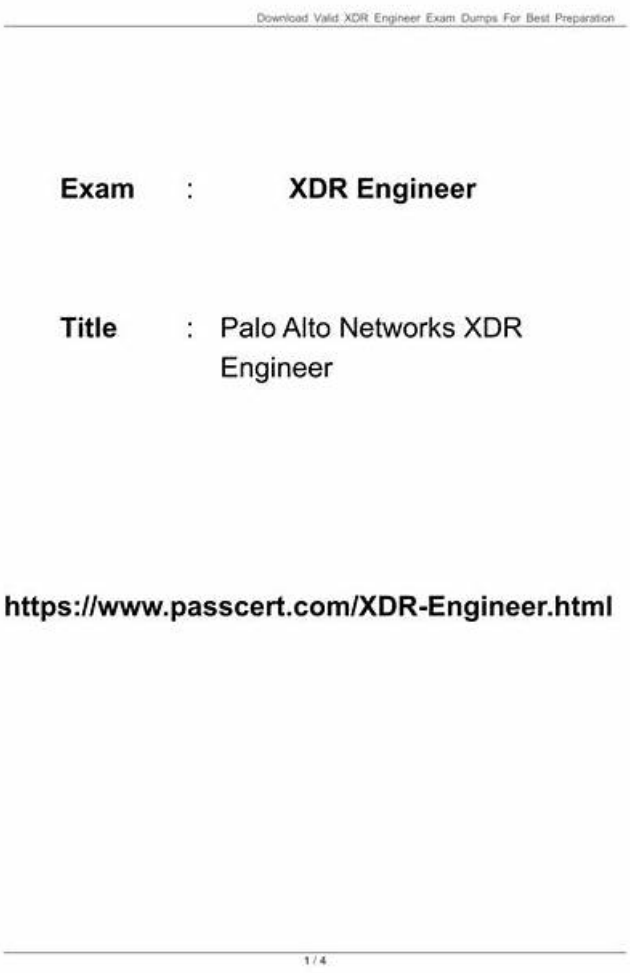
XDR-Engineer Valid Test Format, Download XDR-Engineer Demo



What's more, part of that RealVCE XDR-Engineer dumps now are free: https://drive.google.com/open?id=1iXjUGlyimlcdpkSTR3Jw71fDqLnwL5fT

The XDR-Engineer study braindumps are compiled by our frofessional experts who have been in this career fo r over ten years. Carefully written and constantly updated content of our XDR-Engineer exam questions can make you keep up with the changing direction of the exam, without aimlessly learning and wasting energy. In addition, there are many other advantages of our XDR-Engineer learning guide. Hope you can give it a look and you will love it for sure!

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Maintenance and Troubleshooting: This section of the exam measures skills of the XDR engineer and covers managing software component updates for Cortex XDR, such as content, agents, Collectors, and Broker VM. It also includes troubleshooting data management issues like data ingestion and parsing, as well as resolving issues with Cortex XDR components to ensure ongoing system reliability and performance.

Topic 2	• Detection and Reporting: This section of the exam measures skills of the detection engineer and covers creating detection rules to meet security requirements, including correlation, custom prevention rules, and the use of behavioral indicators of compromise (BIOCs) and indicators of compromise (IOCs). It also assesses configuring exceptions and exclusions, as well as building custom dashboards and reporting templates for effective threat detection and reporting.
Topic 3	• Cortex XDR Agent Configuration: This section of the exam measures skills of the XDR engineer and covers configuring endpoint prevention profiles and policies, setting up endpoint extension profiles, and managing endpoint groups. The focus is on ensuring endpoints are properly protected and policies are consistently applied across the organization.
Topic 4	• Ingestion and Automation: This section of the exam measures skills of the security engineer and covers onboarding various data sources including NGFW, network, cloud, and identity systems. It also includes managing simple automation rules, configuring Broker VM applets and clusters, setting up XDR Collectors, and creating parsing rules for data normalization and automation within the Cortex XDR environment.
Topic 5	• Planning and Installation: This section of the exam measures skills of the security engineer and covers the deployment process, objectives, and required resources such as hardware, software, data sources, and integrations for Cortex XDR. It also includes understanding and explaining the deployment and functionality of components like the XDR agent, Broker VM, XDR Collector, and Cloud Identity Engine. Additionally, it assesses the ability to configure user roles, permissions, and access controls, as well as knowledge of data retention and compute unit considerations.

Palo Alto Networks XDR Engineer Sample Questions (Q37-Q42):

NEW QUESTION # 37
Based on the SBAC scenario image below, when the tenant is switched to permissive mode, which endpoint (s) data will be accessible?

- A. E1 only
- B. E1, E2, and E3
- C. E2 only
- D. E1, E2, E3, and E4

Answer: B

Explanation:
In Cortex XDR,Scope-Based Access Control (SBAC)restricts user access to data based on predefined scopes, which can be assigned to endpoints, users, or other resources. Inpermissive mode, SBAC allows users to access data within their assigned scopes but may restrict access to data outside those scopes. The question assumes an SBAC scenario with four endpoints (E1, E2, E3, E4), where the user likely has access to a specific scope (e.g., Scope A) that includes E1, E2, and E3, while E4 is in a different scope (e.g., Scope B).
* Correct Answer Analysis (C):When the tenant is switched to permissive mode, the user will have access toE1, E2, and E3because these endpoints are within the user's assigned scope (e.g., Scope A).
E4, being in a different scope (e.g., Scope B), will not be accessible unless the user has explicit accessto that scope. Permissive mode enforces scope restrictions, ensuring that only data within the user's scope is visible.
* Why not the other options?
* A. E1 only: This is too restrictive; the user's scope includes E1, E2, and E3, not just E1.

* B. E2 only: Similarly, this is too restrictive; the user's scope includes E1, E2, and E3, not just E2.
* D. E1, E2, E3, and E4: This would only be correct if the user had access to both Scope A and Scope B or if permissive mode ignored scope restrictions entirely, which it does not. Permissive mode still enforces SBAC rules, limiting access to the user's assigned scopes.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains SBAC: "In permissive mode, Scope-Based Access Control restricts user access to endpoints within their assigned scopes, ensuring data visibility aligns with scope permissions" (paraphrased from the Scope-Based Access Control section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers SBAC configuration, stating that "permissive mode allows access to endpoints within a user's scope, such as E1, E2, and E3, while restricting access to endpoints in other scopes" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheet includes "post-deployment management and configuration" as a key exam topic, encompassing SBAC 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 # 38
The most recent Cortex XDR agents are being installed at a newly acquired company. A list with endpoint types (i.e., OS, hardware, software) is provided to the engineer. What should be cross-referenced for the Linux systems listed regarding the OS types and OS versions supported?

- A. Agent Installer Certificate
- B. Kernel Module Version Support
- C. Content Compatibility Matrix
- D. End-of-Life Summary

Answer: B

Explanation:
When installing Cortex XDR agents on Linux systems, ensuring compatibility with the operating system (OS) type and version is critical, especially for the most recent agent versions. Linux systems require specific kernel module support because the Cortex XDR agent relies on kernel modules for core functionality, such as process monitoring, file system protection, and network filtering. TheKernel Module Version Support documentation provides detailed information on which Linux distributions (e.g., Ubuntu, CentOS, RHEL) and kernel versions are supported by the Cortex XDR agent, ensuring the agent can operate effectively on the target systems.
* Correct Answer Analysis (B):TheKernel Module Version Supportshould be cross-referenced for Linux systems to verify that the OS types (e.g., Ubuntu, CentOS) and specific kernel versions listed are supported by the Cortex XDR agent. This ensures that the agent's kernel modules, which are essential for protection features, are compatible with the Linux endpoints at the newly acquired company.
* Why not the other options?
* A. Content Compatibility Matrix: A Content Compatibility Matrix typically details compatibility between content updates (e.g., Behavioral Threat Protection rules) and agent versions, not OS or kernel compatibility for Linux systems.
* C. End-of-Life Summary: The End-of-Life Summary provides information on agent versions or OS versions that are no longer supported by Palo Alto Networks, but it is not the primary resource for checking current OS and kernel compatibility.
* D. Agent Installer Certificate: The Agent Installer Certificate relates to the cryptographic verification of the agent installer package, not to OS or kernel compatibility.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Linux agent requirements: "For Linux systems, cross- reference the Kernel Module Version Support to ensure compatibility with supported OS types and kernel versions" (paraphrased from the Linux Agent Deployment section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers Linux agent installation, stating that "Kernel Module Version Support lists compatible Linux distributions and kernel versions for Cortex XDR agents" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "planning and installation" as a key exam topic, encompassing Linux agent compatibility checks.
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 # 39
A correlation rule is created to detect potential insider threats by correlating user login events from one dataset with file access events from another dataset. The rule must retain all user login events, even if there are no matching file access events, to ensure no login activity is missed.
text
Copy
dataset = x
| join (dataset = y)
Which type of join is required to maintain all records from dataset x, even if there are no matching events from dataset y?

- A. Right
- B. Outer
- C. Left
- D. Inner

Answer: C

Explanation:
In Cortex XDR, correlation rules useXQL (XDR Query Language)to combine data from multiple datasets to detect patterns, such as insider threats. Thejoinoperation in XQL is used to correlate events from two datasets based on a common field (e.g., user ID). The type of join determines how records are matched and retained when there are no corresponding events in one of the datasets. The question specifies that the correlation rule must retainall user login eventsfrom dataset x (the primary dataset containing login events), even if there are no matching file access events in dataset y (the secondary dataset). This requirement aligns with aLeft Join(also called Left Outer Join), which includes all records from the left dataset (dataset x) and any matching records from the right dataset (dataset y). If there is no match in dataset y, the result includes null values for dataset y's fields, ensuring no login events are excluded.
* Correct Answer Analysis (B):ALeft Joinensures that all records from dataset x (user login events) are retained, regardless of whether there are matching file access events in dataset y. This meets the requirement to ensure no login activity is missed.
* Why not the other options?
* A. Inner: An Inner Join only includes records where there is a match in both datasets (x and y).
This would exclude login events from dataset x that have no corresponding file access events in dataset y, which violates the requirement.
* C. Right: A Right Join includes all records from dataset y (file access events) and only matching records from dataset x. This would prioritize file access events, potentially excluding login events with no matches, which is not desired.
* D. Outer: A Full Outer Join includes all records from both datasets, with nulls in places where there is no match. While this retains all login events, it also includes unmatched file access events from dataset y, which is unnecessary for the stated requirement of focusing on login events.
Exact Extract or Reference:
TheCortex XDR Documentation Portalin theXQL Reference Guideexplains join operations: "A Left Join returns all records from the left dataset and matching records from the right dataset. If there is no match, null values are returned for the right dataset's fields" (paraphrased from the XQL Join section). TheEDU-262:
Cortex XDR Investigation and Responsecourse covers correlation rules and XQL, noting that "Left Joins are used in correlation rules to ensure all events from the primary dataset are retained, even without matches in the secondary dataset" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetlists "detection engineering" as a key exam topic, including creating correlation rules with XQL.
References:
Palo Alto Networks Cortex XDR Documentation Portal: XQL Reference Guide (https://docs-cortex.paloaltonetworks.com/)
EDU-262: Cortex XDR Investigation and Response Course Objectives
Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

NEW QUESTION # 40
When isolating Cortex XDR agent components to troubleshoot for compatibility, which command is used to turn off a component on a Windows machine?

- A. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop
- B. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" stop

- C. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp
- D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" runtime stop

Answer: D

Explanation:
Cortex XDR agents on Windows include multiple components (e.g., for exploit protection, malware scanning, or behavioral analysis) that can be individually enabled or disabled for troubleshooting purposes, such as isolating compatibility issues. Thecytool.exeutility, located in the Cortex XDR installation directory (typically C:\Program Files\Palo Alto Networks\Traps\), is used to manage agent components and settings. The runtime stop command specifically disables a component without uninstalling the agent.
* Correct Answer Analysis (B):The command"C:\Program Files\Palo Alto Networks\Traps\cytool.
exe" runtime stopis used to turn off a specific Cortex XDR agent component on a Windows machine.
For example, cytool.exe runtime stop protection would disable the protection component, allowing troubleshooting for compatibility issues while keeping other components active.
* Why not the other options?
* A. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" stop: The xdr.exe binary is not used for managing components; it is part of the agent's corefunctionality. The correct utility is cytool.exe.
* C. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop: Similarly, xdr.exe is not the correct tool, and -s stop is not a valid command syntax for component management.
* D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp: The occp command is not a valid cytool.exe option. The correct command for stopping a component is runtime stop.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains component management: "To disable a Cortex XDR agent component on Windows, use the command cytool.exe runtime stop <component> from the installation directory" (paraphrased from the Troubleshooting section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers agent troubleshooting, stating that "cytool.exe runtime stop is used to turn off specific components for compatibility testing" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing agent component management.
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 # 41
When using Kerberos as the authentication method for Pathfinder, which two settings must be validated on the DNS server? (Choose two.)

- A. DNS forwarders
- B. Reverse DNS zone
- C. Reverse DNS records
- D. AD DS-integrated zones

Answer: B,C

Explanation:
Pathfinderin Cortex XDR is a tool for discovering unmanaged endpoints in a network, often using authentication methods likeKerberosto 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: Areverse DNS zoneis 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:
TheCortex XDR Documentation Portalexplains 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). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers Pathfinder setup, stating that "Kerberos requires valid reverse DNS zones and PTR records for authentication" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "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 # 42
.....

Palo Alto Networks XDR Engineer exam practice questions play a crucial role in Palo Alto Networks XDR Engineer XDR-Engineer exam preparation and give you insights Palo Alto Networks XDR Engineer exam view. You are aware of the Palo Alto Networks XDR Engineer XDR-Engineer exam topics, structure, and a number of the questions that you will face in the upcoming Palo Alto Networks XDR Engineer XDR-Engineer Exam. You can evaluate your Salesforce Palo Alto Networks XDR Engineer exam preparation performance and work on the weak topic areas. But here is the problem where you will get Palo Alto Networks XDR Engineer exam questions.