Study Palo Alto Networks XDR-Engineer Materials & XDR-Engineer Interactive Practice Exam

BONUS!!! Download part of TopExamCollection XDR-Engineer dumps for free: https://drive.google.com/open?id=1VRABLMRq-3dgGjLgiT8u4IFYWc9_CIrX

The customizable Palo Alto Networks XDR-Engineer practice tests create a scenario of a real-based Palo Alto Networks which is helpful for students so they don't feel much pressure when they are giving the final examination. The students can give unlimited XDR-Engineer practice tests and make themselves better day by day to achieve their desired destination. The candidates can even access their previously given Palo Alto Networks XDR-Engineer Practice Test from the history which allows them to be careful while giving the test next time and prepare for Palo Alto Networks XDR-Engineer certification in a better way.

TopExamCollection Palo Alto Networks XDR-Engineer Exam Questions And Answers provide you test preparation information with everything you need. About Palo Alto Networks XDR-Engineer exam, you can find these questions from different web sites or books, but the key is logical and connected. Our questions and answers will not only allow you effortlessly through the exam first time, but also can save your valuable time.

>> Study Palo Alto Networks XDR-Engineer Materials <<

XDR-Engineer Interactive Practice Exam & XDR-Engineer Knowledge Points

As the name suggests,web-based Palo Alto Networks XDR-Engineer practice tests are internet-based. This practice test is appropriate for usage via any operating system such as Mac, iOS, Windows, Android, and Linux which helps you clearing Palo Alto Networks XDR-Engineer exam. All characteristics of the Windows-based CERT NAME practice exam software are available in it which is necessary for Palo Alto Networks XDR-Engineer Exam. No special plugins or software installation is compulsory to attempt the web-based Palo Alto Networks XDR-Engineer practice tests. In addition, the online mock test is supported by all browsers.

Palo Alto Networks XDR Engineer Sample Questions (Q41-Q46):

NEW QUESTION # 41
A multinational company with over 300,000 employees has recently deployed Cortex XDR in North America.
The solution includes the Identity Threat Detection and Response (ITDR) add-on, and the Cortex team has onboarded the Cloud Identity Engine to the North American tenant. After waiting the required soak period and deploying enough agents to receive Identity and threat analytics detections, the team does not see user, group, or computer details for individuals from the European offices.
What may be the reason for the issue?

- A. The ITDR add-on is not compatible with the Cloud Identity Engine
- B. The Cloud Identity Engine needs to be activated in all global regions
- C. The Cloud Identity Engine plug-in has not been installed and configured
- D. The XDR tenant is not in the same region as the Cloud Identity Engine

Answer: D

Explanation:
TheIdentity Threat Detection and Response (ITDR)add-on in Cortex XDR enhances identity-based threat detection by integrating with theCloud Identity Engine, which synchronizes user,group, and computer details from identity providers (e.g., Active Directory, Okta). For the Cloud Identity Engine to provide comprehensive identity data across regions, it must be properly configured and aligned with the Cortex XDR tenant's region.
* Correct Answer Analysis (A):The issue is likely thatthe XDR tenant is not in the same region as the Cloud Identity Engine. Cortex XDR tenants are region-specific (e.g., North America, Europe), and the Cloud Identity Engine must be configured to synchronize data with the tenant in the same region. If the North American tenant is used but the European offices' identity data is managed by a Cloud Identity Engine in a different region (e.g., Europe), the tenant may not receive user, group, or computer details for European users, causing the observed issue.
* Why not the other options?
* B. The Cloud Identity Engine plug-in has not been installed and configured: The question states that the Cloud Identity Engine has been onboarded, implying it is installed and configured.
The issue is specific to European office data, not a complete lack of integration.
* C. The Cloud Identity Engine needs to be activated in all global regions: The Cloud Identity Engine does not need to be activated in all regions. It needs to be configured to synchronize with the tenant in the correct region, and regional misalignment is the more likely issue.
* D. The ITDR add-on is not compatible with the Cloud Identity Engine: The ITDR add-on is designed to work with the Cloud Identity Engine, so compatibility is not the issue.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Cloud Identity Engine integration: "The Cloud Identity Engine must be configured in the same region as the Cortex XDR tenant to ensure proper synchronization of user, group, and computer details" (paraphrased from the Cloud Identity Engine section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers ITDR and identity integration, stating that "regional alignment between the tenant and Cloud Identity Engine is critical for accurate identity data" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing Cloud Identity Engine 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 # 42
Using the Cortex XDR console, how can additional network access be allowed from a set of IP addresses to an isolated endpoint?

- A. Add entries in Exceptions Configuration section of Isolation Exceptions
- B. Add entries in Configuration section of Security Settings
- C. Add entries in the Allowed Domains section of Security Settings for the tenant
- D. Add entries in Response Actions section of Agent Settings profile

Answer: A

Explanation:
In Cortex XDR,endpoint isolationis a response action that restricts network communication to and from an endpoint, allowing only communication with the Cortex XDR management server to maintain agent functionality. To allow additional network access (e.g., from a set of IP addresses) to an isolated endpoint, administrators can configureisolation exceptionsto permit specific traffic while the endpoint remains isolated.
* Correct Answer Analysis (C):TheExceptions Configuration section of Isolation Exceptionsin the Cortex XDR console allows administrators to define exceptions for isolated endpoints, such as permitting network access from specific IP addresses. This ensures that the isolated endpoint can communicate with designated IPs (e.g., for IT support or backup servers) while maintaining isolation from other network traffic.
* Why not the other options?

* A. Add entries in Configuration section of Security Settings: The Security Settings section in the Cortex XDR console is used for general tenant-wide configurations (e.g., password policies), not for managing isolation exceptions.
* B. Add entries in the Allowed Domains section of Security Settings for the tenant: The Allowed Domains section is used to whitelist domains for specific purposes (e.g., agent communication), not for defining IP-based exceptions for isolated endpoints.
* D. Add entries in Response Actions section of Agent Settings profile: The Response Actions section in Agent Settings defines automated response actions (e.g., isolate on specific conditions), but it does not configure exceptions for already isolated endpoints.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains isolation exceptions: "To allow specific network access to an isolated endpoint, add IP addresses or domains in the Exceptions Configuration section of Isolation Exceptions in the Cortex XDR console" (paraphrased from the Endpoint Isolation section). TheEDU-262:
Cortex XDR Investigation and Responsecourse covers isolation management, stating that "Isolation Exceptions allow administrators to permit network access from specific IPs to isolated endpoints" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes
"post-deployment management and configuration" as a key exam topic, encompassing isolation exception configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal: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 # 43
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. Inner
- C. Left
- D. Outer

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 # 44
An XDR engineer is configuring an automation playbook to respond to high-severity malware alerts by automatically isolating the affected endpoint and notifying the security team via email. The playbook should only trigger for alerts generated by the Cortex XDR analytics engine, not custom BIOCs. Which two conditions should the engineer include in the playbook trigger to meet these requirements? (Choose two.)

- A. Alert source is Cortex XDR Analytics
- B. Alert severity is High
- C. Alert category is Malware
- D. Alert status is New

Answer: B,C

Explanation:
In Cortex XDR,automation playbooks(also referred to as response actions or automation rules) allow engineers to define automated responses to specific alerts based on trigger conditions. The playbook in this scenario needs to isolate endpoints and send email notifications for high-severity malware alerts generated by the Cortex XDR analytics engine, excluding custom BIOC alerts. To achieve this, the engineer must configure the playbook trigger with conditions that match the alert's severity, category, and source.
* Correct Answer Analysis (A, C):
* A. Alert severity is High: The playbook should only trigger for high-severity alerts, as specified in the requirement. Setting the conditionAlert severity is Highensures that only alerts with a severity level of "High" activate the playbook, aligning with the engineer's goal.
* C. Alert category is Malware: The playbook targets malware alerts specifically. The condition Alert category is Malwareensures that the playbook only responds to alerts categorized as malware, excluding other types of alerts (e.g., lateral movement, exploit).
* Why not the other options?
* B. Alert source is Cortex XDR Analytics: While this condition would ensure the playbook triggers only for alerts from the Cortex XDR analytics engine (and not custom BIOCs), the requirement to exclude BIOCs is already implicitly met because BIOC alerts are typically categorized differently (e.g., as custom alerts or specific BIOC categories). The alert category (Malware) and severity (High) conditions are sufficient to target analytics-driven malware alerts, and adding the source condition is not strictly necessary for the stated requirements. However, if the engineer wanted to be more explicit, this condition could be considered, but the question asks for the two most critical conditions, which are severity and category.
* D. Alert status is New: The alert status (e.g., New, In Progress, Resolved) determines the investigation stage of the alert, but the requirement does not specify that the playbook should only trigger for new alerts. Alerts with a status of "InProgress" could still be high-severity malware alerts requiring isolation, so this condition is not necessary.
Additional Note on Alert Source: The requirement to exclude custom BIOCs and focus on Cortex XDR analytics alerts is addressed by theAlert category is Malwarecondition, as analytics-driven malware alerts (e.
g., from WildFire or behavioral analytics) are categorized as "Malware," while BIOC alerts are often tagged differently (e.g., as custom rules). If the question emphasized the need to explicitly filter by source, option B would be relevant, but the primary conditions for the playbook are severity and category.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains automation playbook triggers: "Playbook triggers can be configured with conditions such as alert severity (e.g., High) and alert category (e.g., Malware) to automate responses like endpoint isolation and email notifications" (paraphrased from the Automation Rules section).
TheEDU-262: Cortex XDR Investigation and Responsecourse covers playbook creation, stating that
"conditions like alert severity and category ensure playbooks target specific alert types, such as high-severity malware alerts from analytics" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "playbook creation and automation" as a key exam topic, encompassing trigger condition configuration.
References:

Palo Alto Networks Cortex XDR Documentation Portal: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 # 45
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 records
- C. Reverse DNS zone
- 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 # 46
.....

The services provided by our XDR-Engineer test questions are quite specific and comprehensive. First of all, our test material comes from many experts. The gold content of the materials is very high, and the updating speed is fast. By our XDR-Engineer exam prep, you can find the most suitable information according to your own learning needs at any time, and make adjustments and perfect them at any time. Our XDR-Engineer Learning Materials not only provide you with information, and our XDR-Engineer learning guide is tailor-made for you, according to the timetable to study and review.

Our XDR-Engineer : Palo Alto Networks XDR Engineer valid practice torrent mainly provide candidates complete and systematic

studying materials, Easy operation, Without doubt, our XDR-Engineer practice dumps keep up with the latest information and contain the most valued key points that will show up in the real XDR-Engineer exam, If the user fails in the XDR-Engineer exam questions for any reason, we will refund the money after this process.

Joe, do you have a preference between shooting XDR-Engineer for yourself or for clients, To view all the apps in that category, click the category header, Our XDR-Engineer : Palo Alto Networks XDR Engineer valid practice torrent mainly provide candidates complete and systematic studying materials.

Hot Study XDR-Engineer Materials | High-quality XDR-Engineer Interactive Practice Exam: Palo Alto Networks XDR Engineer

Easy operation, Without doubt, our XDR-Engineer practice dumps keep up with the latest information and contain the most valued key points that will show up in the real XDR-Engineer exam.

If the user fails in the XDR-Engineer exam questions for any reason, we will refund the money after this process, If you are still not sure you can pass exams certainly you had better look for valid XDR-Engineer latest dumps.

BTW, DOWNLOAD part of TopExamCollection XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1VRABLMRq-3dgGjLgiT8u4IFYWc9_CIrX