Test XDR-Engineer Engine Version | Valid XDR-Engineer Practice Materials

DOWNLOAD the newest Fast2test XDR-Engineer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ADQnb2ohNxG3QcZZFc7xFPSMiqjv-k-T

By offering the most considerate after-sales services of XDR-Engineer exam torrent materials for you, our whole package services have become famous and if you hold any questions after buying Palo Alto Networks XDR Engineer prepare torrent, get contact with our staff at any time, they will solve your problems with enthusiasm and patience. They do not shirk their responsibility of offering help about XDR-Engineer Test Braindumps for you 24/7 that are wary and considerate for every exam candidate's perspective. Understanding and mutual benefits are the cordial principles of services industry. We know that tenet from the bottom of our heart, so all parts of service are made due to your interests.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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.

Topic 3	• 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 4	• 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 5	• 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.

Valid XDR-Engineer Practice Materials & Practice XDR-Engineer Test

As the old saying goes, Rome was not built in a day. For many people, it's no panic passing the XDR-Engineer exam in a short time. Luckily enough， as a professional company in the field of XDR-Engineer practice questions ,our products will revolutionize the issue. The XDR-Engineer Study Materials that our professionals are compiling which contain the most accurate questions and answers will effectively solve the problems you may encounter in preparing for the XDR-Engineer exam.

Palo Alto Networks XDR Engineer Sample Questions (Q31-Q36):

NEW QUESTION # 31
Which action is being taken with the query below?
dataset = xdr_data
| fields agent_hostname, _time, _product
| comp latest as latest_time by agent_hostname, _product
| join type=inner (dataset = endpoints
| fields endpoint_name, endpoint_status, endpoint_type) as lookup lookup.endpoint_name = agent_hostname
| filter endpoint_status = ENUM.CONNECTED
| fields agent_hostname, endpoint_status, latest_time, _product

- A. Checking for endpoints with outdated agent versions
- B. Monitoring the latest activity of endpoints
- C. Monitoring the latest activity of connected firewall endpoints
- D. Identifying endpoints that have disconnected from the network

Answer: B

Explanation:
The providedXQL (XDR Query Language)query in Cortex XDR retrieves and processes data to provide insights into endpoint activity. Let's break down the query to understand its purpose:
* dataset = xdr_data | fields agent_hostname, _time, _product: Selects thexdr_datadataset (general event data) and retrieves fields for the agent hostname, timestamp, and product (e.g., agent type or component).
* comp latest as latest_time by agent_hostname, _product: Computes the latest timestamp (_time) for each combination of agent_hostname and _product, naming the result latest_time. This identifies the most recent activity for each endpoint and product.
* join type=inner (dataset = endpoints | fields endpoint_name, endpoint_status, endpoint_type) as lookup lookup.endpoint_name = agent_hostname: Performs an inner join with theendpointsdataset, matching endpoint_name (from the endpoints dataset) with agent_hostname (from xdr_data), and retrieves fields like endpoint_status and endpoint_type.
* filter endpoint_status = ENUM.CONNECTED: Filters the results to include only endpoints with a status ofCONNECTED.
* fields agent_hostname, endpoint_status, latest_time, _product: Outputs the final fields: hostname, status, latest activity time, and

product.
* Correct Answer Analysis (A):The query ismonitoring the latest activity of endpoints. It calculates the most recent activity (latest_time) for each connected endpoint (agent_hostname) by joining event data (xdr_data) with endpoint metadata (endpoints) and filtering for connected endpoints. This provides a view of the latest activity for active endpoints, useful for monitoring their status and recent events.
* Why not the other options?
* B. Identifying endpoints that have disconnected from the network: The queryfilters for endpoint_status = ENUM.CONNECTED, so it only includes connected endpoints, not disconnected ones.
* C. Monitoring the latest activity of connected firewall endpoints: The query does not filter for firewall endpoints (e.g., using endpoint_type or _product to specify firewalls). It applies to all connected endpoints, not just firewalls.
* D. Checking for endpoints with outdated agent versions: The query does not retrieve or compare agent version information (e.g., agent_version field); it focuses on the latest activity time.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains XQL queries: "Queries using comp latest and joins with the endpoints dataset can monitor the latest activity of connected endpoints by calculating the most recent event timestamps" (paraphrased from the XQL Reference Guide). TheEDU-262: Cortex XDR Investigation and Responsecourse covers XQL for monitoring, stating that "combining xdr_data and endpoints datasets with a latest computation monitors recent endpoint activity" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "dashboards and reporting" as a key exam topic, encompassing XQL queries for monitoring.
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 # 32
When using Kerberos as the authentication method for Pathfinder, which two settings must be validated on the DNS server? (Choose two.)

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

Answer: A,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 # 33
What is the earliest time frame an alert could be automatically generated once the conditions of a new correlation rule are met?

- A. Between 10 and 20 minutes
- B. Immediately
- C. 5 minutes or less
- D. Between 30 and 45 minutes

Answer: C

Explanation:
In Cortex XDR,correlation rulesare used to detect specific patterns or behaviors by analyzing ingested data and generating alerts when conditions are met. The time frame for alert generation depends on the data ingestion pipeline, the processing latency of the Cortex XDR backend, and the rule's evaluation frequency.
For a new correlation rule, once the conditions are met (i.e., the relevant events are ingested and processed), Cortex XDR typically generates alerts within a short time frame, often5 minutes or less, due to its near-real- time processing capabilities.
* Correct Answer Analysis (C):Theearliest time framefor an alert to be generated is5 minutes or less, as Cortex XDR's architecture is designed to process and correlate events quickly. This accounts for the time to ingest data, evaluate the correlation rule, and generate the alert in the system.
* Why not the other options?
* A. Between 30 and 45 minutes: This time frame is too long for Cortex XDR's near-real-time detection capabilities. Such delays might occur in systems with significant processing backlogs, but not in a properly configured Cortex XDR environment.
* B. Immediately: While Cortex XDR is fast, "immediately" implies zero latency, which is not realistic due to data ingestion, processing, and rule evaluation steps. A small delay (within 5 minutes) is expected.
* D. Between 10 and 20 minutes: This is also too long for the earliest possible alert generation in Cortex XDR, as the system is optimized for rapid detection and alerting.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains correlation rule processing: "Alerts are generated within 5 minutes or less after the conditions of a correlation rule are met, assuming data is ingested and processed in near real-time" (paraphrased from the Correlation Rules section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers detection engineering, stating that "Cortex XDR's correlation engine processes rules and generates alerts typically within a few minutes of event ingestion" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing correlation rule alert generation.
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 # 34
How long is data kept in the temporary hot storage cache after being queried from cold storage?

- A. 24 hours, re-queried to a maximum of 14 days
- B. 24 hours, re-queried to a maximum of 7 days
- C. 1 hour, re-queried to a maximum of 12 hours
- D. 1 hour, re-queried to a maximum of 24 hours

Answer: B

Explanation:
In Cortex XDR, data is stored in different tiers:hot storage(for recent, frequently accessed data),cold storage (for older, less frequently accessed data), and atemporary hot storage cachefor data retrieved from cold storage during queries. When data is

queried from cold storage, it is moved to the temporary hot storage cache to enable faster access for subsequent queries. The question asks how long this data remains in the cache and the maximum duration for re-queries.
* Correct Answer Analysis (B):Data retrieved from cold storage is kept in the temporary hot storage cache for24 hours. If the data is re-queried within this period, it remains accessible in the cache. The maximum duration for re-queries is7 days, after which the data may need to be retrieved from cold storage again, incurring additional processing time.
* Why not the other options?
* A. 1 hour, re-queried to a maximum of 12 hours: These durations are too short and do not align with Cortex XDR's data retention policies for the hot storage cache.
* C. 24 hours, re-queried to a maximum of 14 days: While the initial 24-hour cache duration is correct, the 14-day maximum for re-queries is too long and not supported by Cortex XDR's documentation.
* D. 1 hour, re-queried to a maximum of 24 hours: The 1-hour initial cache duration is incorrect, as Cortex XDR retains queried data for 24 hours.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains data storage: "Data queried from cold storage is cached in hot storage for 24 hours, with a maximum re-query period of 7 days" (paraphrased from the Data Management section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers data retention, stating that "queried cold storage data remains in the hot cache for 24 hours, accessible for up to 7 days with re-queries" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing data storage management.
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 # 35
When onboarding a Palo Alto Networks NGFW to Cortex XDR, what must be done to confirm that logs are being ingested successfully after a device is selected and verified?

- A. Wait for an incident that involves the NGFW to populate
- B. Confirm that the selected device has a valid certificate
- C. Retrieve device certificate from NGFW dashboard
- D. Conduct an XQL query for NGFW log data

Answer: D

Explanation:
When onboarding aPalo Alto Networks Next-Generation Firewall (NGFW)to Cortex XDR, the process involves selecting and verifying the device to ensure it can send logs to Cortex XDR. After this step, confirming successful log ingestion is critical to validate the integration. The most direct and reliable method to confirm ingestion is to query the ingested logs usingXQL (XDR Query Language), which allows the engineer to search for NGFW log data in Cortex XDR.
* Correct Answer Analysis (A):Conduct an XQL query for NGFW log datais the correct action.
After onboarding, the engineer can run an XQL query such as dataset = panw_ngfw_logs | limit 10 to check if NGFW logs are present in Cortex XDR. This confirms that logs are being successfully ingested and stored in the appropriate dataset, ensuring the integration is working as expected.
* Why not the other options?
* B. Wait for an incident that involves the NGFW to populate: Waiting for an incident is not a reliable or proactive method to confirm log ingestion. Incidents depend on detection rules and may not occur immediately, even if logs are beingingested.
* C. Confirm that the selected device has a valid certificate: While a valid certificate is necessary during the onboarding process (e.g., for secure communication), this step is part of the verification process, not a method to confirm log ingestion after verification.
* D. Retrieve device certificate from NGFW dashboard: Retrieving the device certificate from the NGFW dashboard is unrelated to confirming log ingestion in Cortex XDR. Certificates are managed during setup, not for post-onboarding validation.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains NGFW log ingestion validation: "To confirm successful ingestion of Palo Alto Networks NGFW logs, run an XQL query (e.g., dataset = panw_ngfw_logs) to verify that log data is present in Cortex XDR" (paraphrased from the Data Ingestion section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers NGFW integration, stating that "XQL queries are used to validate that NGFW logs are being ingested after onboarding" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing log ingestion validation.
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 # 36
.....

Our customer service is available all day, and your problems can be solved efficiently at any time. Last but not least, we can guarantee the security of the purchase process of XDR-Engineer Test Questions and the absolute confidentiality of customer information. You do not have to worry about these issues, because we know that this is a basic condition for us to establish a good business model. If you have any questions, you can always contact us online or email us. We will reply as soon as possible.

BTW, DOWNLOAD part of Fast2test XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1ADQnb2ohNxG3QcZZFc7xFPSMiqjv-k-T