Study Palo Alto Networks XDR-Engineer Group | Training XDR-Engineer Material

BTW, DOWNLOAD part of Exam4PDF XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1n2943-afV35VxIUpKgam-Zo_GsPK6taZ

All the XDR-Engineer training files of our company are designed by the experts and professors in the field. The quality of our study materials is guaranteed. According to the actual situation of all customers, we will make the suitable study plan for all customers. If you buy the XDR-Engineer learning dumps from our company, we can promise that you will get the professional training to help you pass your exam easily. By our professional training, you will pass your exam and get the related certification in the shortest time.

Our XDR-Engineer practice materials will help you pass the XDR-Engineer exam with ease. The industry experts hired by XDR-Engineer study materials explain all the difficult-to-understand professional vocabularies by examples, diagrams, etc. All the languages used in XDR-Engineer real test were very simple and easy to understand. With our XDR-Engineer Study Materials, you don't have to worry about that you don't understand the content of professional books. You also don't need to spend expensive tuition to go to tutoring class. XDR-Engineer test engine can help you solve all the problems in your study.

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

Training Palo Alto Networks XDR-Engineer Material, New XDR-Engineer Test Tips

The Palo Alto Networks XDR Engineer (XDR-Engineer) practice questions (desktop and web-based) are customizable, meaning users can set the questions and time according to their needs to improve their discipline and feel the real-based exam scenario to pass the Palo Alto Networks XDR-Engineer Certification. Customizable mock tests comprehensively and accurately represent the actual Palo Alto Networks XDR Engineer (XDR-Engineer) certification exam scenario.

Palo Alto Networks XDR Engineer Sample Questions (Q20-Q25):

NEW QUESTION # 20
Which XQL query can be saved as a behavioral indicator of compromise (BIOC) rule, then converted to a custom prevention rule?

- A. dataset = xdr_data
  | filter event_type = ENUM.PROCESS and event_type = ENUM.DEVICE and
  action_process_image_name = "**"
  and action_process_image_command_line = "-e cmd*"
  and action_process_image_command_line != "*cmd.exe -a /c*"
- B. dataset = xdr_data
  | filter event_type = FILE and (event_sub_type = FILE_CREATE_NEW or event_sub_type = FILE_WRITE or

event_sub_type = FILE_REMOVE or event_sub_type = FILE_RENAME) and agent_hostname = "hostname"
| filter lowercase(action_file_path) in ("/etc/*", "/usr/local/share/*", "/usr/share/*") and action_file_extension in ("conf", "txt")
| fields action_file_name, action_file_path, action_file_type, agent_ip_addresses, agent_hostname, action_file_path

- C. dataset = xdr_data
| filter event_type = ENUM.DEVICE and action_process_image_name = "**"
and action_process_image_command_line = "-e cmd*"
and action_process_image_command_line != "*cmd.exe -a /c*"
- D. dataset = xdr_data
| filter event_type = ENUM.PROCESS and action_process_image_name = "**" and action_process_image_command_line = "-e cmd*" and action_process_image_command_line != "*cmd.exe -a /c*"

Answer: D

Explanation:
In Cortex XDR, aBehavioral Indicator of Compromise (BIOC)rule defines a specific pattern of endpoint behavior (e.g., process execution, file operations, or network activity) that can trigger an alert. BIOCs are often created usingXQL (XDR Query Language)queries, which are then saved as BIOC rules to monitor for the specified behavior. To convert a BIOC into acustom prevention rule, the BIOC must be associated with a Restriction profile, which allows the defined behavior to be blocked rather than just detected. For a query to be suitable as a BIOC and convertible to a prevention rule, it must meet the following criteria:
* It must monitor a behavior that Cortex XDR can detect on an endpoint, such as process execution, file operations, or device events.
* The behavior must be actionable for prevention (e.g., blocking a process or file operation), typically involving events like process launches (ENUM.PROCESS) or file modifications (ENUM.FILE).
* The query should not include overly complex logic (e.g., multiple event types with conflicting conditions) that cannot be translated into a BIOC rule.
Let's analyze each query to determine which one meets these criteria:
* Option A: dataset = xdr_data | filter event_type = ENUM.DEVICE ...This query filters for event_type = ENUM.DEVICE, which relates to device-related events (e.g., USB device connections).
While device events can be monitored, the additional conditions (action_process_image_name = "**" and action_process_image_command_line) are process-related attributes, which are typically associated with ENUM.PROCESS events, not ENUM.DEVICE. This mismatch makes the query invalid for a BIOC, as it combines incompatible event types and attributes. Additionally, device events are not typically used for custom prevention rules, as prevention rules focus on blocking processes or fileoperations, not device activities.
* Option B: dataset = xdr_data | filter event_type = ENUM.PROCESS and event_type = ENUM.
DEVICE ...This query attempts to filter for events that are both ENUM.PROCESS and ENUM.
DEVICE (event_type = ENUM.PROCESS and event_type = ENUM.DEVICE), which is logically incorrect because an event cannot have two different event types simultaneously. In XQL, the event_type field must match a single type (e.g., ENUM.PROCESS or ENUM.DEVICE), and combining them with an and operator results in no matches. This makes the query invalid for creating a BIOC rule, as it will not return any results and cannot be used for detection or prevention.
* Option C: dataset = xdr_data | filter event_type = FILE ...This query monitors file-related events (event_type = FILE) with specific sub-types (FILE_CREATE_NEW, FILE_WRITE, FILE_REMOVE, FILE_RENAME) on a specific hostname, targeting file paths (/etc/*, /usr/local/share/*, /usr/share/*) and extensions (conf, txt). While this query can be saved as a BIOC to detect file operations, it is not ideal for conversion to a custom prevention rule. Cortex XDR prevention rules typically focus on blocking process executions (via Restriction profiles), not file operations. While file-based BIOCs can generate alerts, converting them to prevention rules is less common, as Cortex XDR's prevention mechanisms are primarily process-oriented (e.g., terminating a process), not file-oriented (e.g., blocking a file write). Additionally, the query includes complex logic (e.g., multiple sub-types, lowercase() function, fields clause), which may not fully translate to a prevention rule.
* Option D: dataset = xdr_data | filter event_type = ENUM.PROCESS ...This query monitors process execution events (event_type = ENUM.PROCESS) where the process image name matches a pattern (action_process_image_name = "**"), the command line includes -e cmd*, and excludes commands matching *cmd.exe -a /c*. This query is well-suited for a BIOC rule, as it defines a specific process behavior (e.g., a process executing with certain command-line arguments) that Cortex XDR can detect on an endpoint. Additionally, this type of BIOC can be converted to a custom prevention rule by associating it with aRestriction profile, which can block the process execution if the conditions are met. For example, the BIOC can be configured to detect processes with action_process_image_name =
"**" and action_process_image_command_line = "-e cmd*", and a Restriction profile can terminate such processes to prevent the behavior.
Correct Answer Analysis (D):
Option D is the correct choice because it defines a process-based behavior (ENUM.PROCESS) that can be saved as a BIOC rule to detect the specified activity (processes with certain command-line arguments). It can then be converted to a custom prevention rule by adding it to a Restriction profile, which will block the process execution when the conditions are met. The query's conditions are straightforward and compatible with Cortex XDR's BIOC and prevention framework, making it the best fit for the requirement.

Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains BIOC and prevention rules: "XQL queries monitoring process events (ENUM.PROCESS) can be saved as BIOC rules to detect specific behaviors, and these BIOCs can be added to a Restriction profile to create custom prevention rules that block the behavior" (paraphrased from the BIOC and Restriction Profile sections). TheEDU-260: Cortex XDR Prevention and Deployment course covers BIOC creation, stating that "process-based XQL queries are ideal for BIOCs and can be converted to prevention rules via Restriction profiles to block executions" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing BIOC rule creation and conversion to prevention rules.
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 # 21
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 7 days
- B. 24 hours, re-queried to a maximum of 14 days
- C. 1 hour, re-queried to a maximum of 12 hours
- D. 1 hour, re-queried to a maximum of 24 hours

Answer: A

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 # 22
When using Kerberos as the authentication method for Pathfinder, which two settings must be validated on the DNS server? (Choose two.)

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

- D. Reverse DNS zone

Answer: A,D

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 # 23
A query is created that will run weekly via API. After it is tested and ready, it is reviewed in the Query Center. Which available column should be checked to determine how many compute units will be used when the query is run?

- A. Compute Unit Quota
- B. Simulated Compute Units
- C. Query Status
- D. Compute Unit Usage

Answer: D

Explanation:
In Cortex XDR, theQuery Centerallows administrators to manage and reviewXQL (XDR Query Language) queries, including those scheduled to run via API. Each query consumescompute units, a measure of the computational resources required to execute the query. To determine how many compute units a query will use, theCompute Unit Usagecolumn in the Query Center provides the actual or estimated resource consumption based on the query's execution history or configuration.
* Correct Answer Analysis (B):TheCompute Unit Usagecolumn in the Query Center displays the number of compute units consumed by a query when it runs. For a tested and ready query, this column provides the most accurate information on resource usage, helping administrators plan for API-based executions.
* Why not the other options?
* A. Query Status: The Query Status column indicates whether the query ran successfully, failed, or is pending, but it does not provide information on compute unit consumption.
* C. Simulated Compute Units: While some systems may offer simulated estimates, Cortex XDR' s Query Center does not have a "Simulated Compute Units" column. The actual usage is tracked in Compute Unit Usage.
* D. Compute Unit Quota: The Compute Unit Quota refers to the total available compute units for the tenant, not the specific usage

of an individual query.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Query Center functionality: "The Compute Unit Usage column in the Query Center shows the compute units consumed by a query, enabling administrators to assess resource usage for scheduled or API-based queries" (paraphrased from the Query Center section). TheEDU-
262: Cortex XDR Investigation and Responsecourse covers query management, stating that "Compute Unit Usage provides details on the resources used by each query in the Query Center" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing query resource 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 # 24
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. Identifying endpoints that have disconnected from the network
- B. Checking for endpoints with outdated agent versions
- C. Monitoring the latest activity of connected firewall endpoints
- D. Monitoring the latest activity of endpoints

Answer: D

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 # 25
.....

If you are confusing while preparing for your test, you can choose to trust our information resource and experienced experts rather than waste a lot of time on learning aimlessly. Our Palo Alto Networks XDR-Engineer exam guide materials are edited by professional experts based on latest and exact information about the real test. Generally the passing rate is high up to 99.79%. If you want to pass exam as soon as possible, our XDR-Engineer Exam Guide Materials will be most useful product for you.

Training XDR-Engineer Material: https://www.exam4pdf.com/XDR-Engineer-dumps-torrent.html

In this way, you will be able to not only evaluate your progress but also overcome mistakes before the XDR-Engineer actual examination, To see whether our XDR-Engineer training dumps are worthy to buy, you can have a try on our product right now, XDR-Engineer This certification gives us more opportunities, Palo Alto Networks Study XDR-Engineer Group Are you still looking for a job?

Audit collection is enabled on OpsMgr agents XDR-Engineer by running a task in the OpsMgr console, Now we can have a brief look together, In this way, you will be able to not only evaluate your progress but also overcome mistakes before the XDR-Engineer actual examination.

You Need to Trust Palo Alto Networks XDR-Engineer Exam Questions

To see whether our XDR-Engineer training dumps are worthy to buy, you can have a try on our product right now, XDR-Engineer This certification gives us more opportunities.

Are you still looking for a job, We provide our XDR-Engineer practice materials on the superior quality and being confident that they will help you expand your horizon of knowledge of the exam.

- XDR-Engineer Learning Materials - XDR-Engineer Study Guide - XDR-Engineer Test Braindumps □ Easily obtain free download of ☀ XDR-Engineer □☀□ by searching on ✔ www.prep4away.com □✔□ □XDR-Engineer Testing Center
- Renowned XDR-Engineer Learning Quiz display the most useful Exam Brain Dumps - Pdfvce □ Open [www.pdfvce.com] enter 「 XDR-Engineer 」 and obtain a free download □XDR-Engineer Valid Exam Test
- PDF XDR-Engineer Cram Exam □ XDR-Engineer Sample Exam □ Interactive XDR-Engineer Practice Exam □ Search for ➥ XDR-Engineer □ and easily obtain a free download on ➡ www.practicevce.com □□□ ☃XDR-Engineer Testing Center
- XDR-Engineer Learning Engine □ Composite Test XDR-Engineer Price □ XDR-Engineer Dumps Free □ Search for □ XDR-Engineer □ and download exam materials for free through ✔ www.pdfvce.com □✔□ □Composite Test XDR-Engineer Price
- Interactive XDR-Engineer Practice Exam □ PDF XDR-Engineer Cram Exam □ XDR-Engineer Learning Engine □ Easily obtain free download of ✔ XDR-Engineer □✔□ by searching on 「 www.prepawaypdf.com 」 □XDR-Engineer New Learning Materials
- XDR-Engineer Learning Materials - XDR-Engineer Study Guide - XDR-Engineer Test Braindumps □ Search on ➡ www.pdfvce.com □□□ for ▸ XDR-Engineer ◂ to obtain exam materials for free download □XDR-Engineer Sample Exam
- Palo Alto Networks XDR-Engineer Dumps PDF - Pass Exam Immediately (2026) □ Search for 《 XDR-Engineer 》 and download exam materials for free through ▸ www.prepawayete.com ◂ □Reliable XDR-Engineer Exam Topics
- XDR-Engineer Exam Passing Score □ Reliable XDR-Engineer Exam Topics □ Dumps XDR-Engineer Cost □ Download ➡ XDR-Engineer □□□ for free by simply entering ☀ www.pdfvce.com □☀□ website □□XDR-Engineer Exam Cram Pdf
- XDR-Engineer Valid Test Question □ Reliable XDR-Engineer Exam Topics □ Exam Sample XDR-Engineer Online □ Go to website （ www.prep4away.com ） open and search for ➡ XDR-Engineer □□□ to download for free □XDR-Engineer Exam Cram Pdf
- XDR-Engineer Valid Test Question ☑ PDF XDR-Engineer Cram Exam □ New Braindumps XDR-Engineer Book □

Immediately open [www.pdfvce.com] and search for " XDR-Engineer " to obtain a free download □Valid XDR-Engineer Exam Tips

- Pass Guaranteed Quiz Palo Alto Networks - XDR-Engineer - Palo Alto Networks XDR Engineer Authoritative Study Group □ Download ➡ XDR-Engineer □□□ for free by simply searching on ☀ www.pdfdumps.com □☀□ □New Braindumps XDR-Engineer Book
- www.stes.tyc.edu.tw, witpacourses.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.competize.com, stackblitz.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Exam4PDF XDR-Engineer dumps for free: https://drive.google.com/open?id=1n2943-afV35VxIUpKgam-Zo_GsPK6taZ