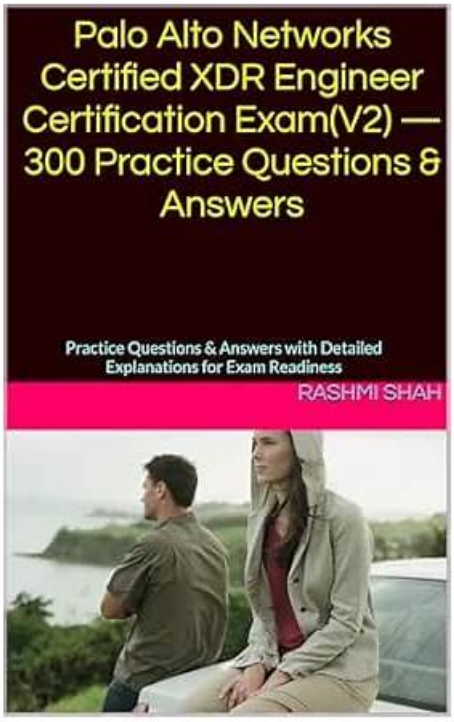
XDR-Engineer Valid Exam Cost - XDR-Engineer Exam Questions



BTW, DOWNLOAD part of Exam4Docs XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1F7aZkyzCduo_HMNfnqfj3805PuAl14h2

Our Palo Alto Networks XDR-Engineer practice exam simulator mirrors the Palo Alto Networks XDR-Engineer exam experience, so you know what to anticipate on Palo Alto Networks XDR Engineer day. Our Palo Alto Networks XDR-Engineer practice test software features various question styles and levels, so you can customize your Palo Alto Networks XDR-Engineer Exam Questions preparation to meet your needs.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Section	Weight	Objectives
Planning and Installation	14%	- User roles, permissions and access control configuration - Data retention and compute unit considerations - Cortex XDR components: Agent, Broker VM, Collector, Cloud Identity Engine - Deployment process, objectives and required resources

Maintenance and Troubleshooting	20%	- Software and content updates management - Data ingestion and parsing troubleshooting - Component troubleshooting: agents, collectors, Broker VM
Cortex XDR Agent Configuration	22%	- Endpoint extension profiles and policies configuration - Endpoint prevention profiles and policies configuration - Endpoint groups management
Detection and Reporting	22%	- Custom dashboards and reporting templates - Correlation rules creation - Exceptions and exclusions setup - IOC and BIOC configuration
Ingestion and Automation	22%	- Simple automation rules management - Broker VM applets and clusters configuration - Onboard data sources: NGFW, network, cloud, identity systems - XDR Collectors configuration - Parsing rules for data normalization

Palo Alto Networks XDR-Engineer PDF Questions Exam Preparation and Study Guide

The only goal of all experts and professors in our company is to design the best and suitable XDR-Engineer study materials for all people. According to the different demands of many customers, they have designed the three different versions of the XDR-Engineer certification study guide materials for all customers: PDF, Soft and APP versions. They sincerely hope that all people who use XDR-Engineer Exam Questions from our company can pass the XDR-Engineer exam and get the related certification successfully. And our pass rate for XDR-Engineer exam questions is high as more than 98%.

Palo Alto Networks XDR Engineer Sample Questions (Q79-Q84):

NEW QUESTION # 79
Which statement describes the functionality of fixed filters and dashboard drilldowns in enhancing a dashboard's interactivity and data insights?

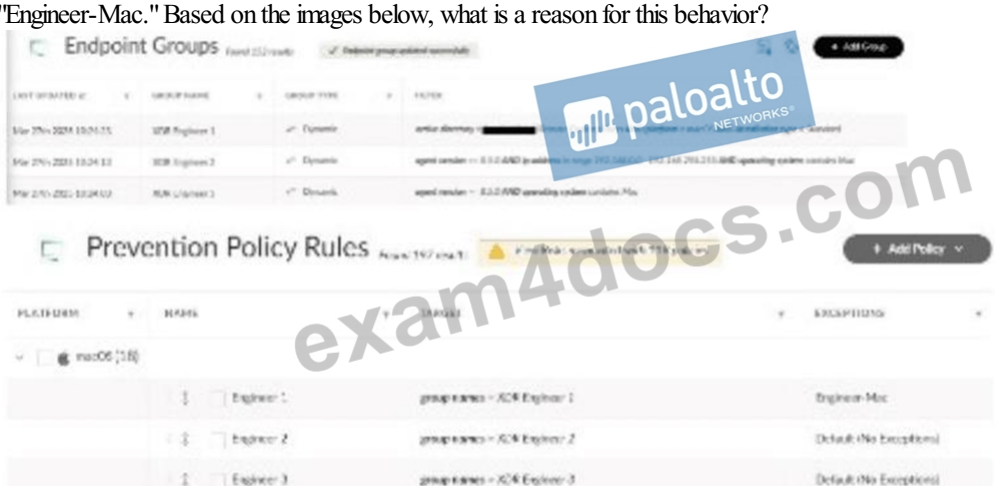
- A. Fixed filters let users select predefined or dynamic values to adjust the scope, while dashboard drilldowns provide interactive insights or trigger contextual changes, like linking to XQL searches
- B. Fixed filters allow users to adjust the layout, while dashboard drilldowns provide links to external reports and/or dashboards
- C. Fixed filters limit the data visible in widgets, while dashboard drilldowns allow users to download data from the dashboard in various formats
- D. Fixed filters allow users to select predefined data values, while dashboard drilldowns enable users to alter the scope of the data displayed by selecting filter values from the dashboard header

Answer: A

Explanation:
In Cortex XDR,fixed filtersanddashboard drilldownsare key features that enhance the interactivity and usability of dashboards. Fixed filters allow users to refine the data displayed in dashboard widgets by selecting predefined or dynamic values (e.g., time ranges, severities, or alertsources), adjusting the scope of the data presented. Dashboard drilldowns, on the other hand, enable users to interact with widget elements (e.
g., clicking on a chart bar) to gain deeper insights, such as navigating to detailed views, other dashboards, or executingXQL (XDR Query Language)searches for granular data analysis.
* Correct Answer Analysis (C):The statement in option C accurately describes the functionality:Fixed filters let users select predefined or dynamic values to adjust the scope, ensuring users can focus on specific subsets of data (e.g., alerts from a particular source).Dashboard drilldowns provide interactive insights or trigger contextual changes, like linking to XQL searches, allowing users to explore related data or perform detailed investigations directly from the dashboard.
* Why not the other options?
* A. Fixed filters allow users to select predefined data values, while dashboard drilldowns enable users to alter the scope of the data displayed by selecting filter values from the dashboard header: This is incorrect because drilldowns do not alter the scope via dashboard header filters; they provide navigational or query-based insights (e.g., linking to XQL searches).

Additionally, fixed filters support both predefined and dynamic values, not just predefined ones.
* B. Fixed filters limit the data visible in widgets, while dashboard drilldowns allow users to download data from the dashboard in various formats: While fixed filters limit data in widgets, drilldowns do not primarily facilitate data downloads. Downloads are handled via export functions, not drilldowns.
* D. Fixed filters allow users to adjust the layout, while dashboard drilldowns provide links to external reports and/or dashboards: Fixed filters do not adjust the dashboard layout; they filter data. Drilldowns can link to other dashboards but not typically to external reports, and their primary role is interactive data exploration, not just linking.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes dashboard features: "Fixed filters allow users to select predefined or dynamic values to adjust the scope of data in widgets. Drilldowns enable interactive exploration by linking to XQL searches or other dashboards for contextual insights" (paraphrased from the Dashboards and Widgets section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers dashboard configuration, stating that "fixed filters refine data scope, and drilldowns provide interactive links to XQL queries or related dashboards" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "dashboards and reporting" as a key exam topic, encompassing fixed filters and drilldowns.
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 # 80
Multiple remote desktop users complain of in-house applications no longer working. The team uses macOS with Cortex XDR agents version 8.7.0, and the applications were previously allowed by disable prevention rules attached to the Exceptions Profile "Engineer-Mac." Based on the images below, what is a reason for this behavior?



- A. Endpoint IP address changed from 192.168.0.0 range to 192.168.100.0 range
- B. XDR agent version was downgraded from 8.7.0 to 8.4.0
- C. The Cloud Identity Engine is disconnected or removed
- D. Installation type changed from VDI to Kubernetes

Answer: A

Explanation:
The scenario involves macOS users with Cortex XDR agents (version 8.7.0) who can no longer run in-house applications that were previously allowed via disable prevention rules in the"Engineer-Mac" Exceptions Profile. This profile is applied to an endpoint group (e.g., "Mac-Engineers"). Theissue likely stems from a change in the endpoint group's configuration or the endpoints' attributes, affecting policy application.
* Correct Answer Analysis (A):The reason for the behavior is that theendpoint IP address changed from 192.168.0.0 range to 192.168.100.0 range. In Cortex XDR, endpoint groups can be defined using dynamic criteria, such as IP address ranges, to apply specific policies like the "Engineer-Mac" Exceptions Profile. If the group "Mac-Engineers" was defined to include endpoints in the 192.168.0.0 range, and the remote desktop users' IP addresses changed to the 192.168.100.0 range (e.g., due to a network change or VPN reconfiguration), these endpoints would no longer belong to the "Mac- Engineers" group. As a result, the "Engineer-Mac" Exceptions Profile, which allowed the in-house applications, would no longer apply, causing the applications to be blocked by default prevention rules.
* Why not the other options?

* B. The Cloud Identity Engine is disconnected or removed: The Cloud Identity Engine provides user and group data for identity-based policies, but it is not directly related to Exceptions Profiles or application execution rules. Its disconnection would not affect the application of the "Engineer-Mac" profile.
* C. XDR agent version was downgraded from 8.7.0 to 8.4.0: The question states the users are using version 8.7.0, and there's no indication of a downgrade. Even if a downgrade occurred, it's unlikely to affect the application of an Exceptions Profile unless specific features were removed, which is not indicated.
* D. Installation type changed from VDI to Kubernetes: The installation type (e.g., VDI for virtual desktops or Kubernetes for containerized environments) is unrelated to macOS endpoints running remote desktop sessions. This change would not impact the application of the Exceptions Profile.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains endpoint group policies: "Dynamic endpoint groups based on IP address ranges apply policies like Exceptions Profiles; if an endpoint's IP changes to a different range, it may no longer belong to the group, affecting policy enforcement" (paraphrased from the Endpoint Management section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers policy application, stating that "changes in IP address ranges can cause endpoints to fall out of a group, leading to unexpected policy behavior like blocking previously allowed applications" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing endpoint group and policy 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 # 81
Which troubleshooting step should be performed first to determine why logs from a third-party firewall do not appear in Cortex XDR?

- A. Disable all other data sources in XDR to isolate the third-party firewall logs, ensuring that no other logs interfere with the ingestion process.
- B. Immediately reset the XDR data ingestion module and clear all stored logs, as reconfiguring the data ingestion pipeline will ensure proper log collection.
- C. Determine whether the firewall's log forwarding settings match the XDR ingestion requirements, ensuring the correctlog format and transport protocol.
- D. Modify the XDR correlation rules to manually import the missing logs, as logs that do not match predefined rules will not be ingested into the system.

Answer: C

Explanation:
The first troubleshooting step is to verify the third-party firewall is forwarding logs in the format and transport method expected by Cortex XDR. If the forwarding format, destination, port, or protocol is incorrect, the logs will not be ingested or parsed properly.

NEW QUESTION # 82
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 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 = 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*"
- 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 = 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

Answer: A

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 # 83
An attacker attempts to dump credentials by accessing LSASS memory on a Windows endpoint.
Which Cortex XDR detection capability is most likely involved?

- A. Process Behavioral Monitoring
- B. Device Profiling
- C. Patch Assessment
- D. Inventory Synchronization

Answer: A

Explanation:
Credential dumping techniques often involve abnormal access to sensitive processes such as LSASS. Behavioral monitoring detects suspicious process interactions, privilege escalation attempts, and memory access patterns commonly associated with credential theft.

NEW QUESTION # 84
.....

All candidates want to get Palo Alto Networks authentication in a very short time, this has developed into an inevitable trend. Each of them is eager to have a strong proof to highlight their abilities, so they have the opportunity to change their current status. It is not easy to qualify for a qualifying exam in such a short period of time. Our company's XDR-Engineer Study Guide is very good at helping customers pass the exam and obtain XDR-Engineer certificate in a short time, and now you can free download the demo of our XDR-Engineer exam torrent from our website. You will love our XDR-Engineer exam prep for sure.

- 2026 XDR-Engineer Valid Exam Cost Free PDF | Professional XDR-Engineer Exam Questions: Palo Alto Networks XDR Engineer □ Easily obtain free download of [XDR-Engineer] by searching on ▹ www.prepawaypdf.com ◃ □New XDR-Engineer Test Tips
- freestyler.ws, onlyfans.com, nguza.com, users.playground.ru, scalar.usc.edu, www.competize.com, telegra.ph, fortunetelleroracle.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, telegra.ph, Disposable vapes

2026 Latest Exam4Docs XDR-Engineer PDF Dumps and XDR-Engineer Exam Engine Free Share: https://drive.google.com/open?id=1F7aZkyzCduo_HMNfnqfj3805PuAl14h2