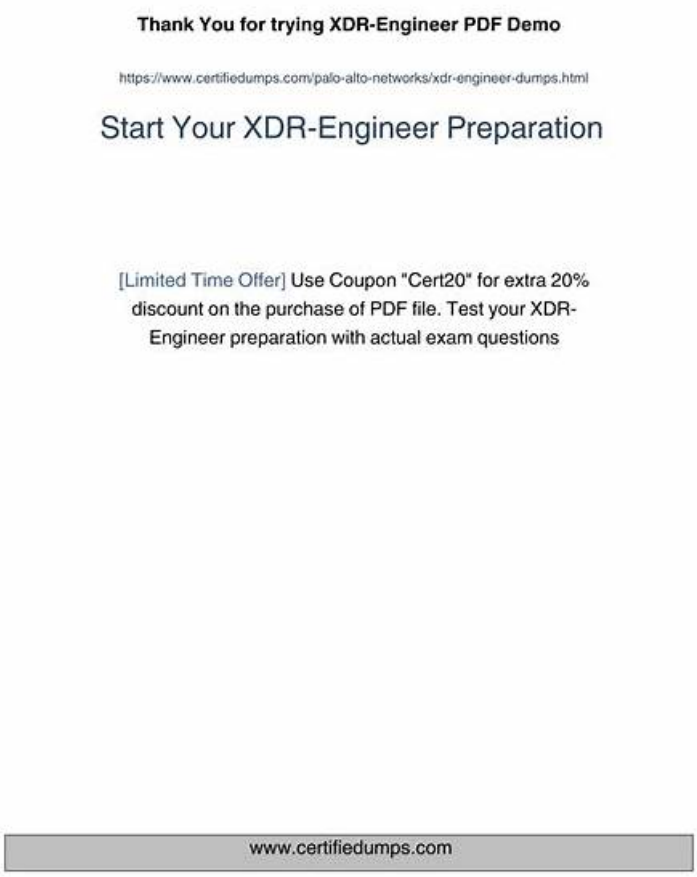
XDR-Engineer Reliable Source & XDR-Engineer Reliable Dumps Questions



P.S. Free 2026 Palo Alto Networks XDR-Engineer dumps are available on Google Drive shared by VerifiedDumps: https://drive.google.com/open?id=1jdkX5b7G1oBj2tG5FQtzXmeq8eAgRg3P

If you want to pass the exam in the shortest time, our XDR-Engineer study materials can help you achieve this dream. Our XDR-Engineer learning quiz according to your specific circumstances, for you to develop a suitable schedule and learning materials, so that you can prepare in the shortest possible time to pass the exam needs everything. If you use our XDR-Engineer training prep, you only need to spend twenty to thirty hours to practice our XDR-Engineer study materials, then you are ready to take the exam and pass it successfully.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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 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.

Express Greetings to a Useful Future by Getting Palo Alto Networks XDR-Engineer Dumps

To get prepared for the Palo Alto Networks XDR Engineer certification exam, applicants face a lot of trouble if the study material is not updated. They are using outdated materials resulting in failure and loss of money and time. So to solve all these problems, VerifiedDumps offers actual XDR-Engineer Questions to help candidates overcome all the obstacles and difficulties they face during XDR-Engineer examination preparation.

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

NEW QUESTION # 37
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 = 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
- D. 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*"

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 # 38
After deploying Cortex XDR agents to a large group of endpoints, some of the endpoints have a partially protected status. In which two places can insights into what is contributing to this status be located? (Choose two.)

- A. Asset Inventory
- B. Management Audit Logs
- C. XQL query of the endpoints dataset
- D. All Endpoints page

Answer: C,D

Explanation:
In Cortex XDR, apartially protected statusfor an endpoint indicates that some agent components or protection modules (e.g., malware protection, exploit prevention) are not fully operational, possibly due to compatibility issues, missing prerequisites, or configuration errors. To troubleshoot this status, engineers need to identify the specific components or issues affecting the endpoint, which can be done by examining detailed endpoint data and status information.
* Correct Answer Analysis (B, C):
* B. XQL query of the endpoints dataset: AnXQL (XDR Query Language)query against the endpoints dataset (e.g., dataset = endpoints | filter endpoint_status = "PARTIALLY_PROTECTED" | fields endpoint_name, protection_status_details) provides detailed insights into the reasons for the partially protected status. The endpoints dataset includes fields like protection_status_details, which specify which modules are not functioning and why.
* C. All Endpoints page: TheAll Endpoints pagein the Cortex XDR console displays a list of all endpoints with their statuses, including those that are partially protected. Clicking into an endpoint's details reveals specific information about the protection status, such as which modules are disabled or encountering issues, helping identify the cause of the status.
* Why not the other options?
* A. Management Audit Logs: Management Audit Logs track administrative actions (e.g., policy changes, agent installations), but they do not provide detailed insights into the endpoint's protection status or the reasons for partial protection.
* D. Asset Inventory: Asset Inventory provides an overview of assets (e.g., hardware, software) but does not specifically detail the protection status of Cortex XDR agents or the reasons for partial protection.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains troubleshooting partially protected endpoints:"Use the All Endpoints page to view detailed protection status, and run an XQL query against the endpoints dataset to identify specific issues contributing to a partially protected status" (paraphrased from the Endpoint Management section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers endpoint troubleshooting, stating that "the All Endpoints page and XQL queries of the endpoints dataset provide insights into partial protection issues" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing endpoint status investigation.
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
What is the earliest time frame an alert could be automatically generated once the conditions of a new correlation rule are met?

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

Answer: B

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 # 40
Based on the Malware profile image below, what happens when a new custom-developed application attempts to execute on an endpoint?

- A. It will not execute
- B. It will immediately execute
- C. It will execute after the second attempt
- D. It will execute after one hour

Answer: A

Explanation:
Since no image was provided, I assume the Malware profile is configured with default Cortex XDR settings, which typically enforce strict malware prevention for unknown or untrusted executables. In Cortex XDR, the Malware profilewithin the security policy determines how executables are handled on endpoints. For anew custom-developed application(an unknown executable not previously analyzed or allow-listed), the default behavior is toblock executionuntil the file is analyzed byWildFire(Palo Alto Networks' cloud-based threat analysis service) or explicitly allowed via policy.
* Correct Answer Analysis (B):By default, Cortex XDR's Malware profile is configured toblock unknown executables, including new custom-developed applications, to prevent potential threats. When the application attempts ilustrator execute, the Cortex XDR agent intercepts it, sends it to WildFire for analysis (if not excluded), and blocks execution until a verdict is received. If the application is not on an allow list or excluded, itwill not executeimmediately, aligning with option B.
* Why not the other options?
* A. It will immediately execute: This would only occur if the application is on an allow list or if the Malware profile is configured to allow unknown executables, which is not typical for default settings.
* C. It will execute after one hour: There is no default setting in Cortex XDR that delays execution for one hour. Execution depends on the WildFire verdict or policy configuration, not a fixed time delay.
* D. It will execute after the second attempt: Cortex XDR does not have a mechanism that allows execution after a second attempt. Execution is either blocked or allowed based on policy and analysis results.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Malware profile behavior: "By default, unknown executables are blocked until a WildFire verdict is received, ensuring protection against new or custom- developed applications" (paraphrased from the Malware Profile Configuration section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers Malware profiles, stating that "default settings block unknown executables to prevent potential threats until analyzed" (paraphrased from course materials).
ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing Malware profile 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
Note on Image: Since the image was not provided, I assumed a default Malware profile configuration. If you can share the image or describe its settings (e.g., specific allow lists, exclusions, or block rules), I can refine the answer to match the exact configuration.

NEW QUESTION # 41
How long is data kept in the temporary hot storage cache after being queried from cold storage?

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

Answer: C

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 # 42
.....

- Pass XDR-Engineer Test Guide Reliable XDR-Engineer Exam Topics Training XDR-Engineer For Exam Download { XDR-Engineer } for free by simply entering ➡ www.vce4dumps.com website Latest XDR-Engineer Test Labs
- Prepare Palo Alto Networks XDR-Engineer Exam To Get Certification Easily obtain free download of （ XDR-Engineer ） by searching on ➡ www.pdfvce.com XDR-Engineer Test Book
- First-rank XDR-Engineer Exam Preparation: Palo Alto Networks XDR Engineer boosts the Most Efficient Training Dumps - www.practicevce.com Download " XDR-Engineer " for free by simply searching on { www.practicevce.com } Exam Dumps XDR-Engineer Demo
- First-rank XDR-Engineer Exam Preparation: Palo Alto Networks XDR Engineer boosts the Most Efficient Training Dumps - Pdfvce Search on [www.pdfvce.com] for { XDR-Engineer } to obtain exam materials for free download XDR-Engineer Valid Exam Question
- Training XDR-Engineer For Exam XDR-Engineer Exam Quizzes Reliable XDR-Engineer Test Cost ➤ www.pdfdumps.com is best website to obtain [XDR-Engineer] for free download Examcollection XDR-Engineer Vce
- XDR-Engineer Passed Pass XDR-Engineer Test Guide Latest XDR-Engineer Practice Questions Search for ✔ XDR-Engineer ✔ and easily obtain a free download on 「 www.pdfvce.com 」 Valid XDR-Engineer Test Voucher
- XDR-Engineer Dumps PDF XDR-Engineer Valid Exam Question Latest XDR-Engineer Practice Questions Go to website www.prepawayete.com open and search for 「 XDR-Engineer 」 to download for free XDR-Engineer Dumps PDF
- Examcollection XDR-Engineer Vce Pass XDR-Engineer Test Guide Training XDR-Engineer For Exam Open ➤ www.pdfvce.com and search for XDR-Engineer to download exam materials for free XDR-Engineer Test Book
- Reliable XDR-Engineer Test Cost XDR-Engineer Exam Quizzes Valid XDR-Engineer Test Voucher Search for ➡ XDR-Engineer and download it for free on " www.easy4engine.com " website XDR-Engineer VCE Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of VerifiedDumps XDR-Engineer dumps for free: https://drive.google.com/open?id=1jdkX5b7G1oBj2tG5FQtzXmeq8eAgRg3P