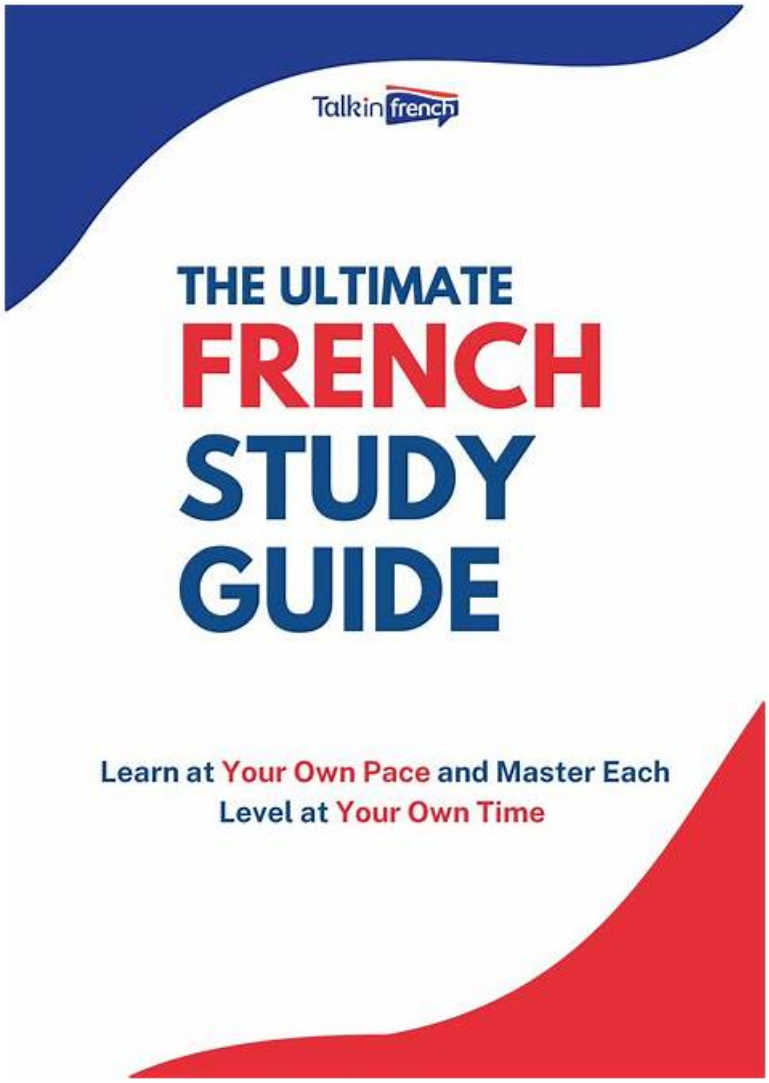
Pass-Sure XDR-Engineer New Study Guide & Leading Offer in Qualification Exams & Marvelous Palo Alto Networks Palo Alto Networks XDR Engineer



2025 Latest ExamPrepAway XDR-Engineer PDF Dumps and XDR-Engineer Exam Engine Free Share: https://drive.google.com/open?id=11QEy6FTXrZ7_EXaqf0o4AId8ahTRe1gq

The Palo Alto Networks XDR Engineer (XDR-Engineer) Exam Questions offered by ExamPrepAway provide you with a good idea of what you can expect in the XDR-Engineer exam from Palo Alto Networks. All the XDR-Engineer exam topics and objectives are well covered by our product. Thus, ExamPrepAway Palo Alto Networks XDR-Engineer Practice Questions are considered a very good resource that will help you in your practicing by focusing on your weak points and strengthening them to easily pass the XDR-Engineer exam.

In addition to the Palo Alto Networks XDR-Engineer PDF dumps, we also offer Palo Alto Networks XDR Engineer practice exam software. You will find the same ambiance and atmosphere when you attempt the real Palo Alto Networks XDR Engineer exam. It will make you practice nicely and productively as you will experience better handling of the Palo Alto Networks XDR-Engineer Questions when you take the actual Palo Alto Networks XDR-Engineer exam to grab the Palo Alto Networks XDR-Engineer certification.

>> XDR-Engineer New Study Guide <<

Newest XDR-Engineer New Study Guide Covers the Entire Syllabus of XDR-Engineer

AS is known to all of us, no pain, no gain. It's also applied in a XDR-Engineer exam, if we want to pass the XDR-Engineer exam, you also need to pay the time, money as well as efforts. However, induction may be quite difficult for someone who have little time to preparing the XDR-Engineer exam. If you face the same problem like this, our product will be your best choice, the practice materials will provide you the most excellent and best ways for the exam. Our product for the XDR-Engineer Exam will help you to save the time as well as grasp the main knoeledge point of the XDR-Engineer exam.

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.

Palo Alto Networks XDR Engineer Sample Questions (Q27-Q32):

NEW QUESTION # 27
Log events from a previously deployed Windows XDR Collector agent are no longer being observed in the console after an OS upgrade. Which aspect of the log events is the probable cause of this behavior?

- A. They are in Winlogbeat format
- B. They are greater than 5MB
- C. They are less than 1MB
- D. They are in Filebeat format

Answer: B

Explanation:
TheXDR Collectoron a Windows endpoint collects logs (e.g., Windows Event Logs) and forwards them to the Cortex XDR console for analysis. An OS upgrade can impact the collector's functionality, particularly if it affects log formats, sizes, or compatibility. If log events are no longer observed after the upgrade, the issue likely relates to a change in how logs are processed or

transmitted. Cortex XDR imposes limits on log event sizes to ensure efficient ingestion and processing.
* Correct Answer Analysis (A):The probable cause is thatthe log events are greater than 5MB. Cortex XDR has a size limit for individual log events, typically around 5MB, to prevent performance issues during ingestion. An OS upgrade may change the way logs are generated (e.g., increasing verbosity or adding metadata), causing events to exceed this limit. If log events are larger than 5MB, the XDR Collector will drop them, resulting in no logs being observed in the console.
* Why not the other options?
* B. They are in Winlogbeat format: Winlogbeat is a supported log shipper for collecting Windows Event Logs, and the XDR Collector is compatible with this format. The format itself is not the issue unless misconfigured, which is not indicated.
* C. They are in Filebeat format: Filebeat is also supported by the XDR Collector for file-based logs. The format is not the likely cause unless the OS upgrade changed the log source, which is not specified.
* D. They are less than 1MB: There is no minimum size limit for log events in Cortex XDR, so being less than 1MB would not cause logs to stop appearing.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains log ingestion limits: "Individual log events larger than 5MB are dropped by the XDR Collector to prevent ingestion issues, which may occur after changes like an OS upgrade" (paraphrased from the XDR Collector Troubleshooting section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers log collection issues, stating that "log events exceeding 5MB are not ingested, a common issue after OS upgrades thatincrease log size" (paraphrased from course materials).
ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing log ingestion issues.
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 # 28
An analyst considers an alert with the category of lateral movement to be allowed and not needing to be checked in the future. Based on the image below, which action can an engineer take to address the requirement?

- A. Create a disable injection and prevention rule for the parent process indicated in the alert
- B. Create an alert exclusion rule by using the alert source and alert name
- C. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement
- D. Create an exception rule for the parent process and the exact command indicated in the alert

Answer: B

Explanation:
In Cortex XDR, alateral movementalert (mapped to MITRE ATT&CK T1021, e.g., Remote Services) indicates potential unauthorized network activity, often involving processes like cmd.exe. If the analyst determines this behavior is allowed (e.g., a legitimate use of cmd /c dir for administrative purposes) and should not be flagged in the future, the engineer needs to suppress future alerts for this specific behavior. The most effective way to achieve this is by creating analert exclusion rule, which suppresses alerts based on specific criteria such as the alert source (e.g., Cortex XDR analytics) and alert name (e.g., "Lateral Movement Detected").
* Correct Answer Analysis (B):Create an alert exclusion rule by using the alert source and alert nameis the recommended action. This approach directly addresses the requirement by suppressing future alerts of the same type (lateral movement) from the specified source, ensuring that this legitimate activity (e.g., cmd /c dir by cmd.exe) does not generate alerts. Alert exclusions can be fine-tuned to apply to specific endpoints, users, or other attributes, making this a targeted solution.
* Why not the other options?
* A. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement: While BIOC suppression rules can suppress specific BIOCs, the alert in question appears to be generated by Cortex XDR analytics (not a custom BIOC), as indicated by the MITRE ATT&CK mapping and alert category. BIOC suppression is more relevant for custom BIOC rules, not analytics-driven alerts.
* C. Create a disable injection and prevention rule for the parent process indicated in the alert: There is no "disable injection and prevention rule" in CortexXDR, and this option does not align with the goal of suppressing alerts. Injection prevention is related to exploit protection, not lateral movement alerts.
* D. Create an exception rule for the parent process and the exact command indicated in the alert: While creating an exception for the parent process (cmd.exe) and command (cmd /c dir) might prevent some detections, it is not the most direct method for suppressing analytics-driven lateral movement alerts. Exceptions are typically used for exploit or malware profiles, not for analytics-based alerts.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains alert suppression: "To prevent future checks for allowed alerts, create an alert exclusion rule using the alert source and alert name to suppress specific alert types" (paraphrased from the Alert Management section). TheEDU-262: Cortex XDR Investigation and Response course covers alert tuning, stating that "alert exclusion rules based on source and name are effective for suppressing analytics-driven alerts like lateral movement" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing alert suppression techniques.
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
Note on Image: The image was not provided, but I assumed a typical lateral movement alert involving a parent process (cmd.exe) and a command (cmd /c dir). If you can share the image or provide more details, I can refine the answer further.

NEW QUESTION # 29
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. Retrieve device certificate from NGFW dashboard
- B. Confirm that the selected device has a valid certificate
- C. Wait for an incident that involves the NGFW to populate
- 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 # 30
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. Query Status
- C. Compute Unit Usage
- D. Simulated Compute Units

Answer: C

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 # 31
A new parsing rule is created, and during testing and verification, all the logs for which field data is to be parsed out are missing. All the other logs from this data source appear as expected. What may be the cause of this behavior?

- A. The Broker VM is offline
- B. The filter stage is dropping the logs
- C. The parsing rule corrupted the database
- D. The XDR Collector is dropping the logs

Answer: B

Explanation:
In Cortex XDR,parsing rulesare used to extract and normalize fields from raw log data during ingestion, ensuring that the data is structured for analysis and correlation. The parsing process includes stages such as filtering, parsing, and mapping. If logs for which field data is to be parsed out are missing, while other logs from the same data source are ingested as expected, the issue likely lies within the parsing rule itself, specifically in the filtering stage that determines which logs are processed.
* Correct Answer Analysis (C):The filter stage is dropping the logsis the most likely cause. Parsing rules often include afilter stagethat determines which logs are processed based on specific conditions (e.
g., log content, source, or type). If the filter stage of the new parsing rule is misconfigured (e.g., using an incorrect condition like log_type != expected_type or a regex that doesn't match the logs), it may drop the logs intended for parsing, causing them to be excluded from the ingestion pipeline. Since other logs from the same data source are ingested correctly, the issue is specific to the parsing rule's filter, not a broader ingestion problem.
* Why not the other options?
* A. The Broker VM is offline: If the Broker VM were offline, it would affect all log ingestion from the data source, not just the specific logs targeted by the parsing rule. The question states that other logs from the same data source are ingested as expected, so the Broker VM is likely operational.
* B. The parsing rule corrupted the database: Parsing rules operate on incoming logs during ingestion and do not directly interact with or corrupt the Cortex XDR database. This is an unlikely cause, and database corruption would likely cause broader issues, not just missing specific logs.
* D. The XDR Collector is dropping the logs: The XDR Collector forwards logs to Cortex XDR, and if it were dropping logs, it would likely affect all logs from the data source, not just those targeted by the parsing rule. Since other logs are ingested correctly, the issue is downstream in the parsing rule, not at the collector level.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains parsing rule behavior: "The filter stage in a parsing rule determines which logs are processed; misconfigured filters can drop logs, causing them to be excluded from ingestion" (paraphrased from the Data Ingestion section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers parsing rule troubleshooting, stating that "if specific logs are missing during parsing, check the filter stage for conditions that may be dropping the logs" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing parsing rule configuration and troubleshooting.
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 # 32
.....

To get respected jobs in tech companies around the globe, hundreds of people take the Palo Alto Networks certification exam every year. Once they clear Palo Alto Networks XDR-Engineer Exam, they easily get jobs and promotions. Hundreds of applicants who appear in the Palo Alto Networks XDR-Engineer Exam don't get a passing score. The major reason behind their failure in the Palo Alto Networks XDR-Engineer Exam is studying the material which is not the latest. So, to save your resources, you must prepare with Palo Alto Networks XDR-Engineer Dumps which has real and updated exam material.

Easily obtain □ XDR-Engineer □ for free download through { www.pdfvce.com } □XDR-Engineer Latest Exam Practice

- Sure XDR-Engineer Pass □ Latest XDR-Engineer Dumps Pdf □ Latest XDR-Engineer Exam Papers □ Search on { www.pass4test.com } for ▹ XDR-Engineer ◃ to obtain exam materials for free download □Latest XDR-Engineer Dumps Pdf
- Eminent XDR-Engineer Training Questions Carry You Subservient Exam Dumps - Pdfvce □ Go to website ✔ www.pdfvce.com □✔□ open and search for 《 XDR-Engineer 》 to download for free □XDR-Engineer Latest Exam Practice
- Reliable XDR-Engineer Exam Tutorial □ New XDR-Engineer Real Test □ New XDR-Engineer Real Test □ Search for □ XDR-Engineer □ and download exam materials for free through ⇛ www.passtestking.com ⇚ □XDR-Engineer Exams Collection
- New XDR-Engineer Study Notes □ VCE XDR-Engineer Dumps □ VCE XDR-Engineer Dumps □ Open website ➠ www.pdfvce.com □ and search for 《 XDR-Engineer 》 for free download □Sure XDR-Engineer Pass
- XDR-Engineer Exams Collection □ VCE XDR-Engineer Dumps □ Latest XDR-Engineer Dumps Pdf □ Download （ XDR-Engineer ） for free by simply entering □ www.pass4leader.com □ website □XDR-Engineer Valid Vce Dumps
- Pass-Sure XDR-Engineer New Study Guide for Real Exam □ Go to website 《 www.pdfvce.com 》 open and search for □ XDR-Engineer □ to download for free □XDR-Engineer Reliable Braindumps
- Valid Test XDR-Engineer Vce Free □ XDR-Engineer Latest Exam Practice □ Sure XDR-Engineer Pass □ Search for 《 XDR-Engineer 》 and easily obtain a free download on ➠ www.real4dumps.com □ □XDR-Engineer Test Centres
- XDR-Engineer Reliable Braindumps □ Latest XDR-Engineer Exam Papers □ Reliable XDR-Engineer Study Plan □ Search for ▸ XDR-Engineer ◂ and download it for free immediately on □ www.pdfvce.com □ ➡□XDR-Engineer Valid Exam Experience
- Quiz 2025 Authoritative Palo Alto Networks XDR-Engineer New Study Guide □ The page for free download of ✔ XDR-Engineer □✔□ on ➡ www.examcollectionpass.com □□□ will open immediately □XDR-Engineer Exam Simulator Online
- adamree449.blogolenta.com, behindvlsi.com, proborton.org, www.stes.tyc.edu.tw, motionentrance.edu.np, adamree449.blogofoto.com, 99tt2.ml30.com, sb.gradxacademy.in, tedcole945.blog-gold.com, Disposable vapes

BTW, DOWNLOAD part of ExamPrepAway XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=11QEy6FTXrZ7_EXaqf0o4AId8ahTRe1gq