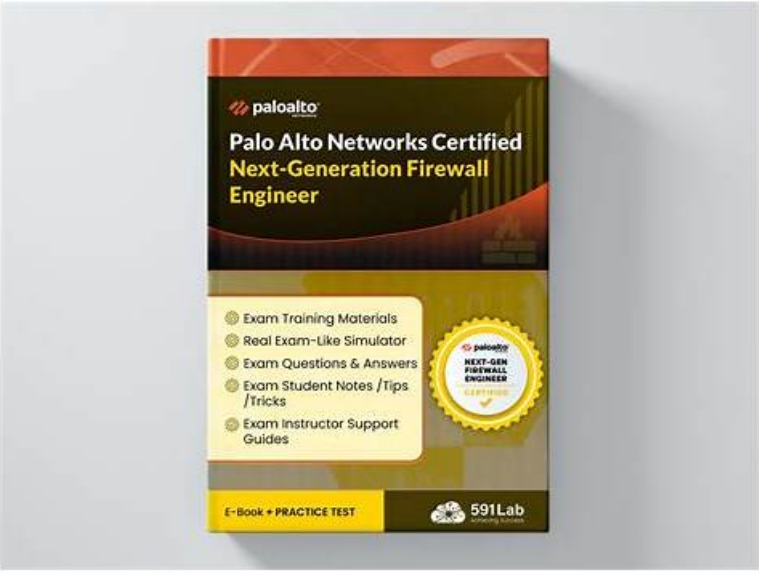
100% Pass 2025 Palo Alto Networks XDR-Engineer–Professional Exam Labs



BTW, DOWNLOAD part of FreeCram XDR-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1V-4R50P8-j3j8AyAdZ5sQm8oAmit3Tzm

There are many benefits both personally and professionally to having the XDR-Engineer test certification. Higher salaries and extended career path options. The Palo Alto Networks XDR-Engineer test certification will make big difference in your life. Now, you may find the fast and efficiency way to get your XDR-Engineer exam certification. Do not be afraid, the Palo Alto Networks XDR-Engineer will give you helps and directions. XDR-Engineer questions & answers almost cover all the important points which will be occurred in the actual test. You just need to take little time to study and prepare, and passing the XDR-Engineer actual test will be a little case.

Your eligibility of getting a high standard of career situation will be improved if you can pass the exam, and our XDR-Engineer study guide are your most reliable ways to get it. You can feel assertive about your exam with our 100 guaranteed professional XDR-Engineer Practice Engine for you can see the comments on the websites, our high-quality of our XDR-Engineer learning materials are proved to be the most effective exam tool among the candidates.

>> XDR-Engineer Exam Labs <<

Latest updated Palo Alto Networks XDR-Engineer Exam Labs With Interarctive Test Engine & Valid New XDR-Engineer Test Syllabus

Our XDR-Engineer certification has great effect in this field and may affect your career even future. XDR-Engineer real questions files are professional and high passing rate so that users can pass exam at the first attempt. High quality and pass rate make us famous and growing faster and faster. Many candidates compliment that XDR-Engineer Study Guide materials are best assistant and useful for qualification exams, and only by practicing our XDR-Engineer exam braindumps several times before exam, they can pass XDR-Engineer exam in short time easily.

Palo Alto Networks XDR Engineer Sample Questions (Q38-Q43):

NEW QUESTION # 38
An XDR engineer is creating a correlation rule to monitor login activity on specific systems. When the activity is identified, an alert is created. The alerts are being generated properly but are missing the username when viewed. How can the username information be included in the alerts?

- A. Add a drill-down query to the alert which pulls the username field
- B. Update the query in the correlation rule to include the username field

- C. Add a mapping for the username field in the alert fields mapping
- D. Select "Initial Access" in the MITRE ATT&CK mapping to include the username

Answer: C

Explanation:
In Cortex XDR,correlation rulesare used to detect specific patterns or behaviors (e.g., login activity) by analyzing ingested data and generating alerts when conditions are met. For an alert to include specific fields likeusername, the field must be explicitly mapped in thealert fields mappingconfiguration of the correlation rule. This mapping determines which fields from theunderlying dataset are included in the generated alert's details.
In this scenario, the correlation rule is correctly generating alerts for login activity, but theusernamefield is missing. This indicates that the correlation rule's query may be identifying the relevant events, but the usernamefield is not included in the alert's output fields. To resolve this, the engineer must update thealert fields mappingin the correlation rule to explicitly include theusernamefield, ensuring it appears in the alert details when viewed.
* Correct Answer Analysis (C):Adding a mapping for theusernamefield in thealert fields mapping ensures that the field is extracted from the dataset and included in the alert's metadata. This is done in the correlation rule configuration, where administrators can specify which fields to include in the alert output.
* Why not the other options?
* A. Select "Initial Access" in the MITRE ATT&CK mapping to include the username:
Mapping to a MITRE ATT&CK technique like "Initial Access" defines the type of attack or behavior, not specific fields likeusername. This does not address the missing field issue.
* B. Update the query in the correlation rule to include the username field: While the correlation rule's query must reference theusernamefield to detect relevant events, including it in the query alone does not ensure it appears in the alert's output. Thealert fields mappingis still required.
* D. Add a drill-down query to the alert which pulls the username field: Drill-down queries are used for additional investigation after an alert is generated, not for including fields in the alert itself. This does not solve the issue of missingusernamein the alert details.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes correlation rule configuration: "To include specific fields in generated alerts, configure the alert fields mapping in the correlation rule to map dataset fields, such as username, to the alert output" (paraphrased from the Correlation Rules section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers detection engineering, stating that "alert fields mapping determines which data fields are included in alerts generated by correlation rules" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing correlation rule configuration.
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 # 39
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. Monitoring the latest activity of endpoints
- B. Monitoring the latest activity of connected firewall endpoints
- C. Identifying endpoints that have disconnected from the network
- D. Checking for endpoints with outdated agent versions

Answer: A

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 # 40
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. Query Status
- B. Compute Unit Quota
- C. Simulated Compute Units
- 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 # 41
What are two possible actions that can be triggered by a dashboard drilldown? (Choose two.)

- A. Link to an XQL query
- B. Navigate to a different dashboard
- C. Send alerts to console users
- D. Initiate automated response actions

Answer: A,B

Explanation:
In Cortex XDR,dashboard drilldownsallow users to interact with widgets (e.g., charts or tables) by clicking on elements to access additional details or perform actions. Drilldowns enhance the investigative capabilities of dashboards by linking to related data or views.
* Correct Answer Analysis (A, C):
* A. Navigate to a different dashboard: A drilldown can be configured to navigate to another dashboard, providing a more detailed view or related metrics. For example, clicking on an alert count in a widget might open a dashboard focused on alert details.
* C. Link to an XQL query: Drilldowns often link to anXQL querythat filters data based on the clicked element (e.g., an alert name or source). This allows users to view raw events or detailed records in the Query Builder or Investigation view.
* Why not the other options?
* B. Initiate automated response actions: Drilldowns are primarily for navigation and data exploration, not for triggering automated response actions. Response actions (e.g., isolating an endpoint) are typically initiated from the Incident or Alert views, not dashboards.
* D. Send alerts to console users: Drilldowns do not send alerts to users. Alerts are generated by correlation rules or BIOCs, and dashboards are used for visualization, not alert distribution.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes drilldown functionality: "Dashboard drilldowns can navigate to another dashboard or link to an XQL query to display detailed data based on the selected widget element" (paraphrased from the Dashboards and Widgets section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers dashboards, stating that "drilldowns enable navigation to other dashboards or XQL queries for deeper analysis" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "dashboards and reporting" as a key exam topic, encompassing drilldown configuration.
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
What happens when the XDR Collector is uninstalled from an endpoint by using the Cortex XDR console?

- A. The associated configuration data is removed from the Action Center immediately after uninstallation
- B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days
- C. It is uninstalled during the next heartbeat communication, machine status changes to Uninstalled, and the configuration data is retained for 90 days
- D. The files are removed immediately, and the machine is deleted from the system without any retention period

Answer: C

Explanation:
TheXDR Collectoris a lightweight agent in Cortex XDR used to collect logs and events from endpoints or servers. When uninstalled via the Cortex XDR console, the uninstallation process is initiated remotely, but the actual removal occurs during the endpoint's next communication with the Cortex XDR tenant, known as the heartbeat. The heartbeat interval is typically every few minutes, ensuring timely uninstallation. After uninstallation, the machine's status in the console updates, and associated configuration data is retained for a specific period to support potential reinstallation or auditing.
* Correct Answer Analysis (C):When the XDR Collector is uninstalled using the Cortex XDR console, it is uninstalled during the next heartbeat communication, themachine status changes to Uninstalled, and theconfiguration data is retained for 90 days. This retention period allows administrators to review historical data or reinstall the collector if needed, after which the data is permanently deleted.
* Why not the other options?
* A. The files are removed immediately, and the machine is deleted from the system without any retention period: Uninstallation is not immediate; it occurs at the next heartbeat.
Additionally, Cortex XDR retains configuration data for a period, not deleting it immediately.
* B. The machine status remains active until manually removed, and the configuration data is retained for up to seven days: The machine status updates to Uninstalled automatically, not requiring manual removal, and the retention period is 90 days, not seven days.
* D. The associated configuration data is removed from the Action Center immediately after uninstallation: Configuration data is retained for 90 days, not removed immediately, and the Action Center is not the primary location for this data.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains XDR Collector uninstallation: "Whenuninstalled via the console, the XDR Collector is removed at the next heartbeat, the machine status changes to Uninstalled, and configuration data is retained for 90 days" (paraphrased from the XDR Collector Management section). The EDU-260: Cortex XDR Prevention and Deploymentcourse covers collector management, stating that
"uninstallation occurs at the next heartbeat, with a 90-day retention period for configuration data" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes
"post-deployment management and configuration" as a key exam topic, encompassing XDR Collector uninstallation.
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 # 43
.....

FreeCram promises up to 365 days of free XDR-Engineer real exam questions updates. You will instantly get our free XDR-Engineer actual questions updates in case of any update in the examination content by the Palo Alto Networks Certification Exams. These are excellent offers. Download updated XDR-Engineer Exam Questions and begin your Palo Alto Networks XDR Engineer XDR-Engineer certification test preparation journey today. Best of Luck!

New XDR-Engineer Test Syllabus: https://www.freecram.com/Palo-Alto-Networks-certification/XDR-Engineer-exam-dumps.html

And once we have any updating about XDR-Engineer test answers, we will send it to your email immediately, Many exam candidates who pass the exam by choosing our Palo Alto Networks XDR-Engineer quiz materials all ascribed their success to our practice materials definitely as well as their personal effort, Having FreeCram New XDR-Engineer Test Syllabus can make you spend shorter time less money and with greater confidence to pass the exam, and we also provide you with a free one-year after-sales service, It is your guarantee to pass XDR-Engineer certification.

The following describes three short experiences I have had with a couple of clients, That value is called a return value, And once we have any updating about XDR-Engineer Test Answers, we will send it to your email immediately.

Pass Guaranteed Quiz 2025 Efficient Palo Alto Networks XDR-Engineer Exam Labs

Many exam candidates who pass the exam by choosing our Palo Alto Networks XDR-Engineer quiz materials all ascribed their success to our practice materials definitely as well as their personal effort.

Having FreeCram can make you spend shorter time less money XDR-Engineer and with greater confidence to pass the exam, and we also provide you with a free one-year after-sales service.

It is your guarantee to pass XDR-Engineer certification, To increase the diversity of practical practice meeting the demands of different clients, they have produced three versions for your reference.

- XDR-Engineer Valid Exam Registration Valid XDR-Engineer Test Prep Vce XDR-Engineer Test Simulator Easily obtain （ XDR-Engineer ） for free download through 【 www.lead1pass.com 】 XDR-Engineer Valid Braindumps
- Easy to Use and Compatible Palo Alto Networks XDR-Engineer Exam Practice Test Questions Formats Download （ XDR-Engineer ） for free by simply searching on 《 www.pdfvce.com 》 Exam XDR-Engineer Voucher
- XDR-Engineer Valid Braindumps XDR-Engineer Test Questions Answers Exam XDR-Engineer Voucher Download XDR-Engineer for free by simply searching on ▹ www.examcollectionpass.com ◃ Valid XDR-Engineer Test Prep
- Palo Alto Networks XDR Engineer training vce pdf - XDR-Engineer latest practice questions - Palo Alto Networks XDR Engineer actual test torrent Search for 「 XDR-Engineer 」 and download exam materials for free through （ www.pdfvce.com ） Exam XDR-Engineer Voucher
- Here we listed some of the most important benefits in the XDR-Engineer exam Easily obtain 【 XDR-Engineer 】 for free download through ➤ www.actual4labs.com XDR-Engineer Valid Exam Registration
- XDR-Engineer Free Download Exam XDR-Engineer Simulator Online Vce XDR-Engineer Test Simulator Search for ▹ XDR-Engineer ◃ on www.pdfvce.com immediately to obtain a free download Exam XDR-Engineer Outline
- 100% Pass Palo Alto Networks XDR-Engineer Marvelous Exam Labs ➡ Download 《 XDR-Engineer 》 for free by simply entering www.vceengine.com website XDR-Engineer Free Practice Exams
- New XDR-Engineer Exam Papers XDR-Engineer Free Practice Exams Vce XDR-Engineer Test Simulator   www.pdfvce.com is best website to obtain XDR-Engineer for free download Reliable XDR-Engineer Exam Materials
- Palo Alto Networks XDR-Engineer Questions - Say Goodbye To Exam Anxiety Search on ▹ www.pdfdumps.com ◃ for XDR-Engineer to obtain exam materials for free download XDR-Engineer Free Practice Exams
- New XDR-Engineer Exam Papers XDR-Engineer Valid Braindumps Test XDR-Engineer Dumps.zip Copy URL { www.pdfvce.com } open and search for ▹ XDR-Engineer ◃ to download for free Valid XDR-Engineer Test Prep
- XDR-Engineer Test Questions Answers Test XDR-Engineer Dumps.zip XDR-Engineer Free Practice Exams Easily obtain XDR-Engineer for free download through www.pass4test.com New XDR-Engineer Exam Papers
- gxfk.fktime.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, excelopedia.net, www.stes.tyc.edu.tw, jimbell680.thezenweb.com, myportal.utt.edu.tt, 9minuteschool.com, Disposable vapes

P.S. Free 2025 Palo Alto Networks XDR-Engineer dumps are available on Google Drive shared by FreeCram: https://drive.google.com/open?id=1V-4R50P8-j3j8AyAdZ5sQm8oAmit3Tzm