

Pass Guaranteed Quiz 2026 Palo Alto Networks XDR-Engineer: Fantastic Palo Alto Networks XDR Engineer Real Exam Answers

Paloalto Networks XDR Engineer Exam

Palo Alto Networks XDR Engineer

<https://www.passquestion.com/xdr-engineer.html>



Pass Paloalto Networks XDR Engineer Exam with PassQuestion
XDR Engineer questions and answers in the first attempt.

<https://www.passquestion.com/>

1 / 5

BONUS!!! Download part of BraindumpsIT XDR-Engineer dumps for free: <https://drive.google.com/open?id=1hCT-phlg9WrpTYSz62EbEE4k3gUYawTm>

If you are quite nervous about the exam, and by chance, you are going to attend the XDR-Engineer exam, then choose the product of our company, because the product of our company will offer you the most real environment for the XDR-Engineer exam, with this it can relieve your nerves while attending the XDR-Engineer exam, as well as strengthen your confidence. Besides the product of our company also provide you plenty of practice materials for you to practice with questions and answers, it will help you to master the key knowledge points as quickly as possible. If you choose the product of our company, passing the XDR-Engineer Exam won't be a dream.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details

Topic 1	<ul style="list-style-type: none"> • 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 2	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • 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 4	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

>> XDR-Engineer Real Exam Answers <<

Valid Palo Alto Networks XDR-Engineer Questions: 100% Authentic [2026]

This kind of polished approach is beneficial for a commendable grade in the Palo Alto Networks XDR Engineer (XDR-Engineer) exam. While attempting the exam, take heed of the clock ticking, so that you manage the Palo Alto Networks XDR-Engineer questions in a time-efficient way. Even if you are completely sure of the correct answer to a question, first eliminate the incorrect ones, so that you may prevent blunders due to human error.

Palo Alto Networks XDR Engineer Sample Questions (Q43-Q48):

NEW QUESTION # 43

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. Update the query in the correlation rule to include the username field
- **B. Add a mapping for the username field in the alert fields mapping**
- C. Add a drill-down query to the alert which pulls the username field
- D. Select "Initial Access" in the MITRE ATT&CK mapping to include the username

Answer: B

Explanation:

In Cortex XDR, correlation rules are 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 like username, the field must be explicitly mapped in the alert fields mapping configuration of the correlation rule. This mapping determines which fields from the underlying dataset are included in the generated alert's details.

In this scenario, the correlation rule is correctly generating alerts for login activity, but the username field is missing. This indicates that the correlation rule's query may be identifying the relevant events, but the username field is not included in the alert's output fields. To resolve this, the engineer must update the alert fields mapping in the correlation rule to explicitly include the username field, ensuring it appears in the alert details when viewed.

* Correct Answer Analysis (C): Adding a mapping for the username field in the alert 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 like username. 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 the username field to detect relevant events, including it in the query alone does not ensure it appears in the alert's output. The alert fields mapping is 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 missing username in the alert details.

Exact Extract or Reference:

The Cortex XDR Documentation Portal describes 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). The EDU-262: Cortex XDR Investigation and Response course covers detection engineering, stating that "alert fields mapping determines which data fields are included in alerts generated by correlation rules" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes "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 # 44

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

Answer: C

NEW QUESTION # 45

During a recent internal purple team exercise, the following recommendation is given to the detection engineering team: Detect and prevent command line invocation of Python on Windows endpoints by non-technical business units. Which rule type should be implemented?

- A. Behavioral Indicator of Compromise (BIOC)
- B. Correlation
- C. Analytics Behavioral Indicator of Compromise (ABIOC)
- D. Indicator of Compromise (IOC)

Answer: A

Explanation:

The recommendation requires detecting and preventing the command line invocation of Python (e.g., python.exe or py.exe) on Windows endpoints, specifically for non-technical business units. This involves identifying a specific behavior (command line execution of Python) and enforcing a preventive action (e.g., blocking the process). In Cortex XDR, Behavioral Indicators of Compromise (BIOCs) are used to define and detect specific patterns of behavior on endpoints, such as command line activities, and can be paired with a Restriction profile to block the behavior.

* Correct Answer Analysis (B): A Behavioral Indicator of Compromise (BIOC) rule should be implemented. The BIOC can be

configured to detect the command line invocation of Python by defining conditions such as the process name (python.exe or py.exe) and the command line arguments.

For example, a BIOC rule might look for process = python.exe with a command line pattern like cmd.

exe /c python*. This BIOC can then be added to a Restriction profile to prevent the execution of Python by non-technical business units, which can be targeted by applying the profile to specific endpoint groups (e.g., those assigned to non-technical units).

* Why not the other options?

* A. Analytics Behavioral Indicator of Compromise (ABIIOC): ABIIOCs are analytics-driven rules generated by Cortex XDR's machine learning and behavioral analytics, not user-defined rules. They are not suitable for creating custom detection and prevention rules like the one needed here.

* C. Correlation: Correlation rules are used to generate alerts by correlating events across multiple datasets (e.g., network and endpoint data), but they do not directly prevent behaviors like command line execution.

* D. Indicator of Compromise (IOC): IOCs are used to detect specific artifacts (e.g., file hashes, IP addresses) associated with known threats, not to detect and prevent behavioral patterns like command line execution.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains BIOC rules: "Behavioral Indicators of Compromise (BIOCs) can detect specific endpoint behaviors, such as command line invocation of processes like Python, and prevent them when added to a Restriction profile" (paraphrased from the BIOC section). The EDU-260:

Cortex XDR Prevention and Deployment course covers detection engineering, stating that "BIOCs are used to detect and block specific behaviors, such as command line executions, on Windows endpoints" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes

"detection engineering" as a key exam topic, encompassing BIOC rule creation.

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 # 46

Using the Cortex XDR console, how can additional network access be allowed from a set of IP addresses to an isolated endpoint?

- A. Add entries in Response Actions section of Agent Settings profile
- B. Add entries in the Allowed Domains section of Security Settings for the tenant
- C. Add entries in Configuration section of Security Settings
- **D. Add entries in Exceptions Configuration section of Isolation Exceptions**

Answer: D

Explanation:

In Cortex XDR, endpoint isolation is a response action that restricts network communication to and from an endpoint, allowing only communication with the Cortex XDR management server to maintain agent functionality. To allow additional network access (e.g., from a set of IP addresses) to an isolated endpoint, administrators can configure isolation exceptions to permit specific traffic while the endpoint remains isolated.

* Correct Answer Analysis (C): The Exceptions Configuration section of Isolation Exceptions in the Cortex XDR console allows administrators to define exceptions for isolated endpoints, such as permitting network access from specific IP addresses. This ensures that the isolated endpoint can communicate with designated IPs (e.g., for IT support or backup servers) while maintaining isolation from other network traffic.

* Why not the other options?

* A. Add entries in Configuration section of Security Settings: The Security Settings section in the Cortex XDR console is used for general tenant-wide configurations (e.g., password policies), not for managing isolation exceptions.

* B. Add entries in the Allowed Domains section of Security Settings for the tenant: The Allowed Domains section is used to whitelist domains for specific purposes (e.g., agent communication), not for defining IP-based exceptions for isolated endpoints.

* D. Add entries in Response Actions section of Agent Settings profile: The Response Actions section in Agent Settings defines automated response actions (e.g., isolate on specific conditions), but it does not configure exceptions for already isolated endpoints.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains isolation exceptions: "To allow specific network access to an isolated endpoint, add IP addresses or domains in the Exceptions Configuration section of Isolation Exceptions in the Cortex XDR console" (paraphrased from the Endpoint Isolation section). The EDU-262:

Cortex XDR Investigation and Response course covers isolation management, stating that "Isolation Exceptions allow administrators to permit network access from specific IPs to isolated endpoints" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes

"post-deployment management and configuration" as a key exam topic, encompassing isolation exception 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 # 47

An engineer is building a dashboard to visualize the number of alerts from various sources. One of the widgets from the dashboard is shown in the image below:

The engineer wants to configure a drilldown on this widget to allow dashboard users to select any of the alert names and view those alerts with additional relevant details. The engineer has configured the following XQL query to meet the requirement:

```
dataset = alerts
```

```
| fields alert_name, description, alert_source, severity, original_tags, alert_id, incident_id
```

```
| filter alert_name =
```

```
| sort desc _time
```

How will the engineer complete the third line of the query (filter alert_name =) to allow dynamic filtering on a selected alert name?

- A. \$x_axis.value
- B. \$x_axis.name
- C. \$y_axis.value
- D. \$y_axis.name

Answer: A

Explanation:

In Cortex XDR, dashboards and widgets support drilldown functionality, allowing users to click on a widget element (e.g., an alert name in a bar chart) to view detailed data filtered by the selected value. This is achieved using XQL (XDR Query Language) queries with dynamic variables that reference the clicked element's value. In the provided XQL query, the engineer wants to filter alerts based on the alert_name selected in the widget.

The widget likely displays alert names along the x-axis (e.g., in a bar chart where each bar represents an alert name and its count). When a user clicks on an alert name, the drilldown query should filter the dataset to show only alerts matching that selected alert_name. In XQL, dynamic filtering for drilldowns uses variables like \$x_axis.value to capture the value of the clicked element on the x-axis.

* Correct Answer Analysis (B): The variable \$x_axis.value is used to reference the value of the x-axis element (in this case, the alert_name) selected by the user. Completing the query with filter alert_name

= \$x_axis.value ensures that the drilldown filters the alerts dataset to show only those records where the alert_name matches the clicked value.

* Why not the other options?

* A. \$y_axis.value: This variable refers to the value on the y-axis, which typically represents a numerical value (e.g., the count of alerts) in a chart, not the categorical alert_name.

* C. \$x_axis.name: This is not a valid XQL variable for drilldowns. XQL uses \$x_axis.value to capture the selected value, not \$x_axis.name.

* D. \$y_axis.name: This is also not a valid XQL variable, and the y-axis is not relevant for filtering by alert_name.

Exact Extract or Reference:

The Cortex XDR Documentation Portal in the XQL Reference Guide explains drilldown configuration: "To filter data based on a clicked widget element, use \$x_axis.value to reference the value of the x-axis category selected by the user" (paraphrased from the Dashboards and Widgets section). The EDU-262: Cortex XDR Investigation and Response course covers dashboard creation and XQL, noting that "drilldown queries use variables like \$x_axis.value to dynamically filter based on user selections" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet lists "dashboards and reporting" as a key exam topic, including configuring interactive widgets.

References:

Palo Alto Networks Cortex XDR Documentation Portal: XQL Reference Guide (<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

