

# Updated XDR-Engineer Testkings & XDR-Engineer Exam Objectives Pdf



BTW, DOWNLOAD part of NewPassLeader XDR-Engineer dumps from Cloud Storage: <https://drive.google.com/open?id=1EaEIsF9L37TBMyl-4JaEz6YWtmfqJV4>

Some candidates may want to get the XDR-Engineer exam braindumps as soon as possible after they buying it, if you also want to get the XDR-Engineer exam braindumps quickly, we can do it for you. You pay for the XDR-Engineer exam dumps, we will send you the downloading link and password to you about five to ten minutes by email. What's more our XDR-Engineer Exam Braindumps is of high quality, it will help you to pass the exam successfully.

XDR-Engineer practice exam will provide you with wholehearted service throughout your entire learning process. This means that unlike other products, the end of your payment means the end of the entire transaction our Palo Alto Networks XDR-Engineer Learning Materials will provide you with perfect services until you have successfully passed the Palo Alto Networks XDR Engineer XDR-Engineer exam.

>> Updated XDR-Engineer Testkings <<

## Palo Alto Networks XDR-Engineer Exam Objectives Pdf & XDR-Engineer Reliable Learning Materials

Failure in the Palo Alto Networks XDR Engineer (XDR-Engineer) exam dumps wastes the money and time of applicants. If you are also planning to take the XDR-Engineer practice test and don't know where to get real XDR-Engineer exam questions, then you are at the right place. NewPassLeader is offering the actual XDR-Engineer Questions that can help you get ready for the examination in a short time. These Palo Alto Networks XDR-Engineer Practice Tests are collected by our team of experts. It has ensured that our questions are genuine and updated. We guarantee that you will be satisfied with the quality of our XDR-Engineer practice questions.

### Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>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.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>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.</li> </ul>

Topic 4	<ul style="list-style-type: none"> <li>• <b>Detection and Reporting:</b> 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.</li> </ul>
Topic 5	<ul style="list-style-type: none"> <li>• <b>Maintenance and Troubleshooting:</b> 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.</li> </ul>

## Palo Alto Networks XDR Engineer Sample Questions (Q18-Q23):

### NEW QUESTION # 18

A correlation rule is created to detect potential insider threats by correlating user login events from one dataset with file access events from another dataset. The rule must retain all user login events, even if there are no matching file access events, to ensure no login activity is missed.

text

Copy

dataset = x

| join (dataset = y)

Which type of join is required to maintain all records from dataset x, even if there are no matching events from dataset y?

- **A. Left**
- B. Inner
- C. Right
- D. Outer

**Answer: A**

Explanation:

In Cortex XDR, correlation rules use XQL (XDR Query Language) to combine data from multiple datasets to detect patterns, such as insider threats. The join operation in XQL is used to correlate events from two datasets based on a common field (e.g., user ID). The type of join determines how records are matched and retained when there are no corresponding events in one of the datasets. The question specifies that the correlation rule must retain all user login events from dataset x (the primary dataset containing login events), even if there are no matching file access events in dataset y (the secondary dataset). This requirement aligns with a Left Join (also called Left Outer Join), which includes all records from the left dataset (dataset x) and any matching records from the right dataset (dataset y). If there is no match in dataset y, the result includes null values for dataset y's fields, ensuring no login events are excluded.

\* Correct Answer Analysis (B): A Left Join ensures that all records from dataset x (user login events) are retained, regardless of whether there are matching file access events in dataset y. This meets the requirement to ensure no login activity is missed.

\* Why not the other options?

\* A. Inner: An Inner Join only includes records where there is a match in both datasets (x and y).

This would exclude login events from dataset x that have no corresponding file access events in dataset y, which violates the requirement.

\* C. Right: A Right Join includes all records from dataset y (file access events) and only matching records from dataset x. This would prioritize file access events, potentially excluding login events with no matches, which is not desired.

\* D. Outer: A Full Outer Join includes all records from both datasets, with nulls in places where there is no match. While this retains all login events, it also includes unmatched file access events from dataset y, which is unnecessary for the stated requirement of focusing on login events.

Exact Extract or Reference:

The Cortex XDR Documentation Portal in the XQL Reference Guide explains join operations: "A Left Join returns all records from the left dataset and matching records from the right dataset. If there is no match, null values are returned for the right dataset's fields" (paraphrased from the XQL Join section). The EDU-262:

Cortex XDR Investigation and Response course covers correlation rules and XQL, noting that "Left Joins are used in correlation rules to ensure all events from the primary dataset are retained, even without matches in the secondary dataset" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet lists "detection engineering" as a key exam topic, including creating correlation rules with XQL.

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>

**NEW QUESTION # 19**

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

**Answer: A**

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 # 20**

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 XDR Collector is dropping the logs

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

**Answer: B**

Explanation:

In Cortex XDR, parsing rules are 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 logs is the most likely cause. Parsing rules often include a filter stage that 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:

The Cortex XDR Documentation Portal explains 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). The EDU-260: Cortex XDR Prevention and Deployment course 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). The Palo Alto Networks Certified XDR Engineer datasheet includes "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 # 21

What will enable a custom prevention rule to block specific behavior?

- **A. A custom behavioral indicator of compromise (BIOC) added to a Restriction profile**
- B. A custom behavioral indicator of compromise (BIOC) added to an Exploit profile
- C. A correlation rule added to an Agent Blocking profile
- D. A correlation rule added to a Malware profile

**Answer: A**

Explanation:

In Cortex XDR, custom prevention rules are used to block specific behaviors or activities on endpoints by leveraging Behavioral Indicators of Compromise (BIOCs). BIOCs define patterns of behavior (e.g., specific process executions, file modifications, or network activities) that, when detected, can trigger preventive actions, such as blocking a process or isolating an endpoint. These BIOCs are typically associated with a Restriction profile, which enforces blocking actions for matched behaviors.

\* Correct Answer Analysis (C): A custom behavioral indicator of compromise (BIOC) added to a Restriction profile enables a custom prevention rule to block specific behavior. The BIOC defines the behavior to detect (e.g., a process accessing a sensitive file), and the Restriction profile specifies the preventive action (e.g., block the process). This configuration ensures that the identified behavior is blocked on endpoints where the profile is applied.

\* Why not the other options?

\* A. A correlation rule added to an Agent Blocking profile: Correlation rules are used to generate alerts by correlating events across datasets, not to block behaviors directly. There is no

"Agent Blocking profile" in Cortex XDR; this is a misnomer.

\* B. A custom behavioral indicator of compromise (BIOC) added to an Exploit profile:

Exploit profiles are used to detect and prevent exploit-based attacks (e.g., memory corruption), not general behavioral patterns defined by BIOCs. BIOCs are associated with Restriction profiles for blocking behaviors.

\* D. A correlation rule added to a Malware profile: Correlation rules do not directly block behaviors; they generate alerts. Malware profiles focus on file-based threats (e.g., executables analyzed by WildFire), not behavioral blocking via BIOCs.

Exact Extract or Reference:

The Cortex XDR Documentation Portal explains BIOC and Restriction profiles: "Custom BIOCs can be added to Restriction profiles to block specific behaviors on endpoints, enabling tailored prevention rules" (paraphrased from the BIOC and Restriction Profile sections). The EDU-260: Cortex XDR Prevention and Deployment course covers prevention rules, stating that "BIOCs in Restriction profiles enable blocking of specific endpoint behaviors" (paraphrased from course materials). The Palo Alto Networks Certified XDR Engineer datasheet includes "detection engineering" as a key exam topic, encompassing BIOC and prevention rule configuration.

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 # 22

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. Simulated Compute Units
- **C. Compute Unit Usage**
- D. Query Status

**Answer: C**

Explanation:

In Cortex XDR, the Query Center allows administrators to manage and review XQL (XDR Query Language) queries, including those scheduled to run via API. Each query consumes compute units, a measure of the computational resources required to execute the query. To determine how many compute units a query will use, the Compute Unit Usage column in the Query Center provides the actual or estimated resource consumption based on the query's execution history or configuration.

\* Correct Answer Analysis (B): The Compute Unit Usage column 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:

The Cortex XDR Documentation Portal explains 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). The EDU-

262: Cortex XDR Investigation and Response course 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). The Palo Alto Networks Certified XDR Engineer datasheet includes "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>

