Download Palo Alto Networks XDR-Engineer Exam Dumps Free

Shared by Harding on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

[Data Ingestion and Integration]

An administrator wants to employ reusable rules within custom parsing rules to apply consistent log field extraction across multiple data sources. Which section of the parsing rule should the administrator use to define those reusable rules in Cortex XDR?

Options:

A- RULE
B- INGEST
C- FILTER
D- CONST

Answer:

D

Question 2

Question Type: MultipleChoice

[Data Ingestion and Integration]

A multinational company with over 300,000 employees has recently deployed Cortex XDR in North Americ

a. The solution includes the Identity Threat Detection and Response (ITDR) add-on, and the Cortex team has onboarded the Cloud Identity Engine to the North American tenant. After waiting the required soak period and deploying enough agents to receive Identity and threat analytics detections, the team does not see user, group, or computer details for individuals from the European offices. What may be the reason for the issue?

Options:

A- The XDR tenant is not in the same region as the Cloud Identity Engine
B- The Cloud Identity Engine plug-in has not been installed and configured
C- The Cloud Identity Engine needs to be activated in all global regions
D- The ITDR add-on is not compatible with the Cloud Identity Engine

Answer:

A

Question 3

Question Type: MultipleChoice

[Data Ingestion and Integration]

Which method will drop undesired logs and reduce the amount of data being ingested?

Options:

A- [COLLECT:vendor='vendor', product='product', target_brokers='', no_hit=drop] * drop _raw_log contains 'undesired logs';
B- [INGEST:vendor='vendor', product='product', target_dataset='vendor_product_raw',no_hit=drop] * filter _raw_log not contains 'undesired logs';
C- [COLLECT:vendor='vendor', product='product', target_dataset='', no_hit=drop] * drop _raw_log contains 'undesired logs';
D- [INGEST:vendor='vendor', product='product', target_brokers='vendor_product_raw', no_hit=keep] * filter _raw_log not contains 'undesired logs';

Answer:

C

Question 4

Question Type: MultipleChoice

[Dashboards and Reporting]

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

Options:

A- Monitoring the latest activity of endpoints
B- Identifying endpoints that have disconnected from the network
C- Monitoring the latest activity of connected firewall endpoints
D- Checking for endpoints with outdated agent versions

Answer:

A

Question 5

Question Type: MultipleChoice

[Data Ingestion and Integration]

Which configuration profile option with an available built-in template can be applied to both Windows and Linux systems by using XDR Collector?

Options:

A- Filebeat
B- HTTP Collector template
C- XDR Collector settings
D- Winlogbeat

Answer:

A

Question 6

Question Type: MultipleChoice

[Cortex XDR Agent Configuration]

A security audit determines that the Windows Cortex XDR host-based firewall is not blocking outbound RDP connections for certain remote workers. The audit report confirms the following:

All devices are running healthy Cortex XDR agents.

A single host-based firewall rule to block all outbound RDP is implemented.

The policy hosting the profile containing the rule applies to all Windows endpoints.

The logic within the firewall rule is adequate.

Further testing concludes RDP is successfully being blocked on all devices tested at company HQ.

Network location configuration in Agent Settings is enabled on all Windows endpoints.What is the likely reason the RDP connections are not being blocked?

Options:

A- The profile's default action for outbound traffic is set to Allow
B- The pertinent host-based firewall rule group is only applied to external rule groups
C- Report mode is set to Enabled in the report settings under the profile configuration
D- The pertinent host-based firewall rule group is only applied to internal rule groups

Answer:

D

Question 7

Question Type: MultipleChoice

[Detection Engineering]

What is the earliest time frame an alert could be automatically generated once the conditions of a new correlation rule are met?

Options:

A- Between 30 and 45 minutes
B- Immediately
C- 5 minutes or less

D- Between 10 and 20 minutes

Answer:

C

Question 8

Question Type: MultipleChoice

[Cortex XDR Agent Configuration]

A static endpoint group is created by adding 321 endpoints using the Upload From File feature. However, after group creation, the members count field shows 244 endpoints. What are two possible reasons why endpoints were not added to the group? (Select two.)

Options:

A- Static groups have a limit of 250 endpoints when adding by file
B- Endpoints added to the new group were previously added to an existing group
C- Endpoints added to the group were in Disconnected or Connection Lost status when groupmembership was added
D- The IP address, hostname, or alias of the endpoints must match an existing agent that has registered with the tenant

Answer:

C, D

Question 9

Question Type: MultipleChoice

[Maintenance and Troubleshooting]

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

Options:

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

C- 24 hours, re-queried to a maximum of 14 days
D- 1 hour, re-queried to a maximum of 24 hours

Answer:

B

P2P exams