



TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>
support@virtulearner.com

Palo Alto Networks

XDR-Engineer

Palo Alto Networks Certified
XDR Engineer Exam

QUESTION: 1

[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?

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

Answer(s): D

QUESTION: 2

[Data Ingestion and Integration]

What will be the output of the function below?

`L_TRIM("a* aapple", "a")`

- A. ' aapple'
- B. " aapple"
- C. "pple"
- D. " aapple-"

Answer(s): A

QUESTION: 3

[Data Ingestion and Integration]

How can a customer ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration?

- A. Activate Windows Event Collector (WEC)
- B. Install the XDR Collector
- C. Enable HTTP collector integration
- D. Install the Cortex XDR agent

Answer(s): B

QUESTION: 4

[Cortex XDR Agent Configuration]

How are dynamic endpoint groups created and managed in Cortex XDR?

- A. Endpoint groups require intervention to update the group with new endpoints when a new device is added to the network
- B. Each endpoint can belong to multiple groups simultaneously, allowing different security policies to be applied to the same device at the same time
- C. After an endpoint group is created, its assigned security policy cannot be changed without deleting and recreating the group
- D. Endpoint groups are defined based on fields such as OS type, OS version, and network

segment

Answer(s): D

QUESTION: 5

[Dashboards and Reporting]

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

Answer(s): B

QUESTION: 6

[Detection Engineering]

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?