KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **XDR Engineer**

Title : Palo Alto Networks XDR Engineer

Version : DEMO

1.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: D

2.What will be the output of the function below?
L_TRIM("a* aapple", "a")
A. ' aapple'
B. " aapple"
C. "pple"
D. " aapple-"
Answer: A

3.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: B

4.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: D

5.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: B