CERTSWARRIOR

IBM

C1000-139
IBM Security QRadar SIEM V7.4.3 Analysis

Questions & Answers PDF

For More Information:

https://www.certswarrior.com/

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

Which step is required for the migration of Ariel data from an old appliance to a new appliance?

A. "Remove all searches created on the old appliance."
B. "Ensure that the destination appliance has enough space to move the data to it. (Correct)"
C. "Remove all the data located on the old appliance."
D. "Ensure that the destination appliance has internet connectivity."

Answer: B

Question: 2

A QRadar analyst was asked to provide a selection of events for further investigation by somebody who does not have access to the QRadar system. Which of these approaches provides an accurate copy of the required data in a readable format?

A. "By using the Advanced Search option in the Log Activity tab, run an AQL command: COPY(SELECT * FROM events LAST 2 HOURS) TO 'output_events.csv' WITH CSV."
B. "By using the Log Activity tab, filter the events until only those that you require are shown. Then, from the Actions list, select Export to CSV > Full Export (All Columns) to download a ZIP file. (Correct)"
C. "By using the \"Event Export (with AQL)\" option in the Log Activity tab, test your query with the Test button. Then, to run the export, click Export to CSV."
D. "Log in to the Command Line Interface and use the ACP tool (/opt/qradar/bin/runjava.sh com.q1labs.ariel.io.ACP) with the necessary AQL filters and destination directory."

Answer: B

Question: 3

Which of these procedures duplicates a report from the Reports tab?

A. "Click Actions, then select the report to duplicate from the pop-up window. Click Duplicate and type a new name for the report."
B. "Select the report to duplicate. From the Actions list, click Duplicate and type a new name for the report. (Correct)"
C. "Click Action > Duplicate Report. Select the report to duplicate and click Finish."
D. "Right-click the report to duplicate. Click Duplicate and type a new name for the report."

Answer: B

Explanation:
Select the report to duplicate. From the Actions list, click Duplicate and type a new name for the report.

Question: 4

Reports can be organized into groups for efficient utilization. What report groups are available by default in QRadar?

A. "Compliance, Executive, Log Sources, Network Management, Security, VoIP, Other (Correct)"
B. "Compliance, Container, Log Sources, Network Management, Security, VoIP, Other"
C. "Compliance, Chart type, Log Sources, Network Management, Security, VoIP, Other"
D. "Compliance, Content, Log Sources, Network Management, Security, VoIP, Other"

Answer: A

Explanation:
By default, the Reports tab displays the list of all reports, however, you can categorize reports into groups such as:
• Compliance
• Executive
• Log Sources
• Network Management
• Security
• VoIP
• Other

Question: 5

How many default dashboards are available in Qradar

A. 4
B. 7
C. 6
D. 5

Answer: D

Explanation:
These are five default dashboard available in Qradar
1. Application Overview .
2. Compliance Overview

3. Network Overview
4. System Monitoring
5. Threat and Security Monitoring

Question: 6

Analysts can filter searches in QRadar from which three (3) of these locations?

A. "Admin search pages"
B. "Log Activity toolbar (Correct)"
C. "Network Activity toolbar (Correct)"
D. "Reports search pages"
E. "Add Filter dialog (Correct)"
F. "Dashboard Activity toolbar"

Answer: B,C,E

Question: 7

Consider this description: Edit the and when either the source or destination IP is one of the following test to include the broadcast addresses of the network. This change removes false positive events that might be caused by the use of broadcast messages. What type of editable building blocks is described?

A. "BB:NetworkDefinition: Broadcast Address Space (Correct)"
B. "BB:NetworkDefinition: Darknet Addresses"
C. "BB:NetworkDefinition: Server Networks"
D. "BB:NetworkDefinition: DLP Addresses"

Answer: Answer: A

Question: 8

What demarcation is added to a custom event property to let you know that this value is held in memory for a set amount of time?

A. "Tabulated"
B. "Indexed (Correct)"
C. "Stored"
D. "Catalogued"

Answer: B

Explanation:
• An index is a set of items that specify information about data in a file and its location in the file system.
• The Index Management feature also provides statistics, such as:
1. The percentage of saved searches running in your deployment that include the indexed property
2. The volume of data that is written to the disk by the index during the selected time frame

Question: 9

What are the search options available for searching offense data on the By Networks page?

A. "Domain, Destination IP, Magnitude, and Events/Flows"
B. "Source IP, Magnitude, VA Risk, and Domain"
C. "Network, Magnitude, VA Risk, and Events/Flows"
D. "Source IP, Destination IP, Events/Flows, and Magnitude (Correct)"

Answer: D

Question: 10

What are unknown events?

A. "None of the above"
B. "The event is collected and parsed, but cannot be mapped or categorized to a specific log source. (Correct)"
C. "The event cannot be understood or parsed by Qradar"
D. "Both of the above"

Answer: B

Explanation:
• The event is collected and parsed, but cannot be mapped or categorized to a specific log source. Log sources that aren't automatically discovered are typically identified as an unknown event log until a log source is manually created in the system.
• When an event cannot be associated to a log source, the event is assigned to a generic log source.
• You can identify these events by searching for events that are associated with the SIM Generic log source or by using the Event is Unparsed filter.

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

http://www.certswarrior.com

Discount Coupon Code:

CERTSWARRIOR10

We Accept

PayPal