Vendor:IBM

Exam Code:C1000-018

Exam Name:IBM QRadar SIEM V7.3.2 Fundamental Analysis

Version: Demo

QUESTION 1

An analyst needs to use a new custom property in a rule.

What must be the mandatory characteristic of the custom property?

A. It must be shared.

B. It must be boolean.

C. It must be stored.

D. It must be extracted.

Correct Answer: B

QUESTION 2

How many normalized timestamp field(s) does an event contain?

A. 2

B. 3

C. 4

D. 1

Correct Answer: B

Explanation:

There are 3 timestamp fields on events in Qradar.

Reference: https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-differenttime-stamps-for-qradar-events?language=en_US

QUESTION 3

An analyst had been researching an Offense that has now disappeared from the active Offense list.

What is the period of time that has to pass before an active Offense that receives no new contributing events or flows become inactive?

A. 5 days

B. 3 days

C. 24 hours

D. 1 hour

Correct Answer: A

Explanation:

An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the

five-day counter is reset.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

---

QUESTION 4

An analyst has to perform an export of events within a timeframe, but not all the columns are present in the log view for the time period the analyst has selected. The analyst only needs specific columns exported for an external analysis.

How can the analyst accomplish this task?

A. Edit the search and select the extra columns, then export the result with Action/Export to XML/Full Export. This export is only supported in XML.

B. Edit the search and select the extra columns, then export the result with Action/Export to XML/Visible Columns. This export is only supported in XML.

C. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Full Export.

D. Edit the search result and select the extra columns, then export the result with Action/Export to CSV/ Visible Columns.

Correct Answer: D

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigation-exporting-events

---

QUESTION 5

What information is included in flow details but is not in event details?

A. Log source information

B. Number of bytes and packets transferred

C. Network summary information

D. Magnitude information

Correct Answer: C

Explanation:

Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other

data, into flow records, which effectively are records of network sessions between two hosts.

Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=overview-qradar-events-flows

---

QUESTION 6

An analyst needs to map a geographic location on all the internal IP addresses.

Which option defines the functions where the analyst can-setup a geographic location of the network object in Network Hierarchy?

A. GPS location and Map

B. Group and IP address

C. Log Activity and Network Activity

D. Longitude and Latitude

Correct Answer: B

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=tasks-network-hierarchy

---

QUESTION 7

The administrator had set up several scheduled reports that can be executed by analysts every Monday, and the first day of each month. On Thursday, an executive requests one of the weekly reports.

If the analyst executes the report on Thursday, what information will the report contain?

A. Data from Monday to Sunday from the previous week.

B. Data from Thursday from the previous week to Wednesday from the current week.

C. Data from Monday to Thursday from the current week.

D. Data from Monday to Wednesday from the current week.

Correct Answer: C

QUESTION 8

An analyst needs to find events coming from unparsed log sources in the Log Activity tab. What is the log source type of unparsed events?

A. SIM Generic

B. SIM Unparsed

C. SIM Error

D. SIM Unknown

Correct Answer: A

Explanation:

SIM Generic log source or by using the Event is Unparsed filter.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=problems-troubleshooting-dsms

---

QUESTION 9

What is the purpose of Anomaly detection rules?

A. They inspect other QRadar rules.

B. They detect if QRadar is operating at peak performance and error free.

C. They detect unusual traffic patterns in the network from the results of saved flow and events.

D. They run past events and flows through the Custom Rules Engine (CRE) to identify threats or security incidents that already occurred.

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/jsa7.4.0/jsa-users-guide/topics/concept/conceptjsa-user-anomaly-detection-rules.html#:~:text=Anomaly%20detection%20rules%20test%20the,patterns%20occur%20in%20your%20network.andtext=Typically%20the%20search%20needs%20to,%2C%

20thresholds%2C%20or%20behavior%20changes

QUESTION 10

Why would an analyst update host definition building blocks in QRadar?

A. To reduce false positives.

B. To narrow a search.

C. To stop receiving events from the host.

D. To close an Offense

Correct Answer: D

Explanation:

Building blocks to reduce the number of offenses that are generated by high volume traffic servers.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=phase-qradar-building-blocks

---

QUESTION 11

An analyst needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter

B. List of test conditions

C. Rule actions

D. Rule responses

Correct Answer: A

QUESTION 12

An analyst noticed that from a particular subnet (203.0.113.0/24), all IP addresses are simultaneously

trying to reach out to the company\\'s publicly hosted FTP server.

The analyst also noticed that this activity has resulted in a Type B Superflow on the Network Activity tab.

Under which category, should the analyst report this issue to the security administrator?

A. Syn Flood

B. Port Scan

C. Network Scan

D. DDoS

Correct Answer: A