C1000-018$^{\text{Q\&As}}$

IBM QRadar SIEM V7.3.2 Fundamental Analysis

QUESTION 1

An analyst observed a port scan attack on an internal network asset from a remote network. Which filter would be useful to determine the compromised host?

A. Any IP

B. Destination IP [Indexed]

C. Source or Destination IP

D. Source IP [Indexed]

Correct Answer: A

QUESTION 2

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 3

An analyst is investigating a series of events that triggered an Offense. The analyst wants to get more detailed information about the IP address from the reference set.

How can the analyst accomplish this?

A. Click on Searches tab then perform an Advanced Search

B. Click on Log Activity tab then perform a Quick Search

C. Click on Searches tab then perform a Quick Search

D. Click on Log Activity tab then perform an Advanced Search

Correct Answer: A

QUESTION 4

An analyst needs to investigate why an Offense was created. How can the analyst investigate?

A. Review the Offense summary to investigate the flow and event details.

B. Review the X-Force rules to investigate the Offense flow and event details.

C. Review pages of the Asset tab to investigate Offense details.

D. Review the Vulnerability Assessment tab to investigate Offense details.

Correct Answer: A

QUESTION 5

What information is displayed in the default “Log Activity” page? (Choose two.)

A. QID

B. Protocol

C. Qmap

D. Log Source

E. Event Name

Correct Answer: DE

QUESTION 6

What is a valid offense naming mechanism? This information should:

A. set the naming of the associated offense(s).

B. set or replace the naming of the associated offense(s).

C. replace the naming of the associated offense(s).

D. be included in the naming of the associated offense(s).

Correct Answer: A

Explanation:

Under "Offense Naming", check "This information should

contribute to the name of the associated offense(s)".

Reference: https://www.ibm.com/support/pages/apar/IJ27086

QUESTION 7

An auditor has requested a report for all Offenses that have happened in the past month. This report generates at the end of every month but the auditor needs to have it for a meeting that is in the middle of the month.

What will happen to the scheduled report if the analyst manually generates this report?

A. The scheduled report needs to be reconfigured.

B. The analyst needs to delete the scheduled report and create a new one.

C. The report will get duplicated so the analyst can then run one manually.

D. The report still generates on the schedule initially configured.

Correct Answer: B

Explanation: Shared schedules must be deleted manually using the Schedules page in the web portal or the Shared Schedules folder in Management Studio. If you delete a shared schedule that is in use, all references to it are replaced with report-specific schedules. If you delete a shared schedule that is used by multiple reports and subscriptions, the report server will create individual schedules for each report and subscription that previously used the shared schedule. Each new individual schedule will contain the date, time, and recurrence pattern that was specified in the shared schedule. Note that Reporting Services does not provide central management of individual schedules. If you delete a shared schedule, you will now have to maintain the schedule information for each individual item.

Reference: https://docs.microsoft.com/en-us/sql/reporting-services/subscriptions/create-modify-anddelete-schedules?view=sql-server-ver15

QUESTION 8

What could be a possible reason that events are routed directly to storage by the custom rule engine (CRE)?

A. System is under high load

B. A rule is processing 20,000 EPS

C. Event normalization issue

D. Event Parsing issue

Correct Answer: A

QUESTION 9

An analyst needs to perform a Quick search to find events under the Log Activity tab that contains an ‘exe’ file during a certain time period.

How can the analyst do this?

A. On the Search bar select Quick Filter, then insert filter criteria for ‘/*.exe/’ and then select a time interval from the view option\\'s drop down.

B. Select Search – New Search from the menu bar, then select all the search criteria required from the UI options provided.

C. Select Quick Searches on the menu bar, then go through the list of saved searches available to see if one already exists, that can be altered.

D. On the Search bar select Quick Filter, insert: ‘exe, last 1 hour’ into the filter criteria, then click Search.

Correct Answer: A

Reference: https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters

QUESTION 10

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