IBM.C1000-018.v2022-05-09.q43

Exam Code:	C1000-018
Exam Name:	IBM QRadar SIEM V7.3.2 Fundamental Analysis
Certification Provider:	IBM
Free Question Number:	43
Version:	v2022-05-09
# of views:	1013
# of Questions views:	430
https://www.exam-tests.com/C1000-018-exam/IBM.C1000-018.v2022-05-09.q43.html	

NEW QUESTION: 1
While creating a new custom property, which is a valid property types selection?
A. AQL Based
B. Event Based
C. Regular Expressions Based
D. Flow Based
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
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).
Answer: A (LEAVE A REPLY)
Explanation
Under "Offense Naming", check "This information should
contribute to the name of the associated offense(s)".

NEW QUESTION: 3
What is the difference between a Quick Search and an Advanced Search?
A. An Advanced Search uses a saved search, while a Quick Search uses a query language.
B. A Quick Search displays results by column, while an Advanced Search displays results by Category.
C. A Quick Search uses a saved search, while an Advanced Search requires a query language.

D. An Advanced Search displays results by Category, while a Quick Search displays results by column.

Answer: C (LEAVE A REPLY)

Explanation

Quick Search

Use the search box to quickly find documents by any keyword or criteria. Here you can also view and re-use your most recent and saved searches.

Advanced Searching

The advanced search allows you to build structured queries using the Jira Query Language.

NEW QUESTION: 4

An analyst for a particular offense needs to investigate to understand the breakdown of the offense details.

How can the analyst do this?

A. Look at the magnitude information and its breakdown.

B. View the attack path of the offense.

C. Look at all the event QIDs attached to the offense.

D. Look at the list of categories, event low level categories and the events attached.

Answer: (SHOW ANSWER)

Magnitude	The Magnitude graph provides a visual representation of how the magnitude was calculated, based on relevance, credibility, and severity. Click the graph to see a detailed description of how the magnitude is calculated.

NEW QUESTION: 5

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

A. Magnitude information

B. Network summary information

C. Number of bytes and packets transferred

D. Log source information

Answer: B (LEAVE A REPLY)

NEW QUESTION: 6

When an Offense is triggered, it only shows the events that triggered the Offense. The analyst wants to investigate further to see more events around the incident, not only those that triggered the Offense. The analyst clicks on the event count and sees the events belonging to the Offense.

How can the analyst processed to see a more detailed picture of what occurred?

A. Right-click on the source IP, and choose More Options, then Information, and then Search Events

B. Right-click on the destination IP, and choose More Options, then Raw Events.

C. Right-click on the source IP, and choose View in DSM Editor.

D. Right-click and filter on the Destination IP.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Which QRadar timestamp specifies when the event was received from the log source?
A. Collect time
B. Start time
C. Storage time
D. Log Source time
Answer: (SHOW ANSWER)
Explanation
https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-different-time-stamps-for-q

NEW QUESTION: 8
An analyst wants to analyze the long-term trending of data from a search.
Which chart would be used to display this data on a dashboard?
A. Scatter Chart
B. Pie Chart
C. Bar Graph
D. Time Series chart
Answer: C (LEAVE A REPLY)
Explanation
You could use a bar graph if you want to track change over time as long as the changes are significant.

NEW QUESTION: 9
The Network Hierarchy is an important part of the system configuration. It can be used to tune out a large number of False Positive Offenses from the standard QRadar rules.
What is the Network Hierarchy?
A. The Network Hierarchy can be used in all Rules and is accessed from the False Positive button in the Network Activity Tab.
B. The Network Hierarchy can be used only in Flow Rules and is accessed from the False Positive button in the Network Activity Tab.
C. There are separate Network Hierarchies for Flow and Event Rules. They are accessed from the False Positive button in the corresponding Activity Tab.
D. The Network Hierarchy can be used in section of the Admin Tab. accessed from the System Configuration.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10

An analyst has observed that for a particular user, authentication to an organization's critical server is different than the normal access pattern.
How can the analyst verify that all the authentications initiated from the user are valid?
A. Perform a search with filter Destination IP group by Username, then validate the Username
B. Perform a search with filter Source IP group by Username, then validate the Username
C. Perform a search with filter Username group by Source IP, then validate the Source IP
D. Perform a search with filter Username group by Source IP, then validate the Destination IP
Answer: (SHOW ANSWER)

NEW QUESTION: 11
When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?
A. When the source is [local or remote]
B. When the destination is [local or remote]
C. When the event(s) were detected by one or more of [these log sources]
D. When an event matches all of the following [Rules or Building Blocks]
Answer: A (LEAVE A REPLY)

NEW QUESTION: 12
After working with an Offense, an analyst set the Offense as hidden. What does the analyst need to do to view the Offense at a later time?
A. Click Clear Filter next to the "Exclude Hidden Offenses".
B. In the all Offenses view, at the top of the view, select "Show hidden" from the "Select an option" drop- down.
C. In the al Offenses view, select Actions, then select show hidden Offenses.
D. Search for all Offenses owned by the analyst
Answer: A (LEAVE A REPLY)
Explanation
To clear the filter on the offense list, click Clear Filter next to the Exclude Hidden Offenses search parameter.

NEW QUESTION: 13
What is the procedure to re-open a closed Offense?
A. A closed Offense cannot be re-opened.
B. Wait for new events/flows that will re-open the closed Offense.
C. Activate the Offense in the action/re-open drop down menu of the Offense tab.
D. Activate the Offense in action/re-open drop down menu in the Admin tab.
Answer: A (LEAVE A REPLY)
Explanation
Not possible to reopen a closed offense.

NEW QUESTION: 14
An analyst has been asked to search for a firewall device that was assigned to a specific address range in the past week.
What method can the analyst use to perform the search that uses simple words or phrases?
A. Export the event data and import it to the spreadsheet for searching.
B. Write a search query using the Ariel Query Language and regex.
C. Use Quick Filter to perform the search for event data.
D. Utilize the Natural Language Query module for searching event data.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 16
QRadar collects information from numerous log sources and other agents. Sometimes these agents stop reporting to QRadar for a variety of reasons. There is a default rule in QRadar to help identify these cases called the Device Stopped Sending Events (DSSE) Rule.
What does the DSSE Rule do?
A. It checks for Rules which have fired due to an absence of Events.
B. It runs when there is an absence of Events.
C. It listens for log sources that send out regular health events and triggers the Rule when encountered
D. It checks for log sources which are reporting that they have not had any communication in a certain amount of time.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
An analyst has been asked to present a report of all the incidents that have been detected by QRadar in the last
24 hours.
How can the analyst achieve this?
A. Create a Common saved search from the last 24 hours and then using the Reports tab, create a report to make use of the existing saved search.
B. Create an Event saved search from the last 24 hours and then using the Log Activity tab, create a report to make use of the existing saved search.
C. Create an Offense saved search from the last 24 hours and then using the Reports tab, create a report to make use of the existing saved search.
D. Create an Event saved search from the last 24 hours and then using the Reports tab, create a report to make use of the existing saved search.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
An analyst needs to investigate why an Offense was created.
How can the analyst investigate?
A. Review the Vulnerability Assessment tab to investigate Offense details.
B. Review pages of the Asset tab to investigate Offense details.
C. Review the Offense summary to investigate the flow and event details.
D. Review the X-Force rules to investigate the Offense flow and event details.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
When is the rating of an Offense magnitude re-evaluated?
A. when a port is opened
B. when new events are added to the Offens
C. when the threat assessment changes
D. when the number of vulnerabilities increases
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.
How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Information, and then DNS Lookup
B. Right-click on the destination address, More Options, then IP Owner
C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup
D. Right-click on the destination address, More Options, then Navigate, and then Destination Summary
Answer: D (LEAVE A REPLY)
Explanation
Navigate > View Destination Summary Displays the offenses that are associated with the selected destination IP address.

NEW QUESTION: 21
An analyst is searching for a list of events that meet specific search criteria and wants to display only the source IP and destination IP information for the events.
To get the required information, the analyst can open the Log Activity tab and then:
A. select advanced search.
type the corresponding AQL query,
then click search.
B. select search,
then new search,
scroll down and select time range, column definitions, the search parameters then click search.
C. click add filter,
select the desired parameters, operators, values and field names,
then click search.
D. select the field names,
select the start and end time from the drop down fields in the filters section, then click search.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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 Log Activity tab then perform an Advanced Search
B. Click on Searches tab then perform a Quick Search
C. Click on Searches tab then perform an Advanced Search
D. Click on Log Activity tab then perform a Quick Search
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23

An analyst has created a custom property from the events for searching for critical information. The analyst also needs to reduce the number of event logs and data volume that is searched when looking for the critical information to maintain the efficiency and performance of QRadar. Which feature should the analyst use?

A. Log Management

B. Database Management

C. Index Management

D. Event Management

Answer: D (LEAVE A REPLY)

NEW QUESTION: 24

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

A. Network summary information

B. Magnitude information

C. Number of bytes and packets transferred

D. Log source information

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 25

What event information within an offense would provide the analyst with a deep insight as to how it was created?

A. Event Magnitude

B. Event QID

C. Event Category

D. Event Payload

Answer: A (LEAVE A REPLY)

NEW QUESTION: 26

An analyst working with QRadar SIEM has been assigned a new Offense and is preparing a custom report on the Offense summary page. From this page, the analyst wants to navigate to the Log Activity or Network Activity page to export the Event/Flow data (Action -> export to CSV). How can the analyst do this? (Choose two)

A. Click the View Attack Path icon.

B. Click the Events / Flows icon.

C. Click the Summary icon.

D. In the Source IP(s) session, click the link to open the page.

E. In the Event/Flow count section, click the link to open the page.

Answer: (SHOW ANSWER)

NEW QUESTION: 27
An analyst wants to analyze the long-term trending of data from a search.
Which chart would be used to display this data on a dashboard?
A. Time Series chart
B. Pie Chart
C. Scatter Chart
D. Bar Graph
Answer: (SHOW ANSWER)

NEW QUESTION: 28
What is the maximum time period for 3 subsequent events to be coalesced?
A. 10 minutes
B. 10 seconds
C. 5 minutes
D. 60 seconds
Answer: B (LEAVE A REPLY)
Explanation
Event coalescing starts after three events have been found with matching properties within a 10 second window.

NEW QUESTION: 29
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. Select Search - New Search from the menu bar, then select all the search criteria required from the UI options provided.
B. 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.
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.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
While creating a new custom property, which is a valid property types selection?
A. Regular Expressions Based
B. Event Based
C. Flow Based

D. AQL Based
Answer: A (LEAVE A REPLY)

NEW QUESTION: 31
What is the purpose of Anomaly detection rules?
A. They inspect other QRadar rules.
B. They run past events and flows through the Custom Rules Engine (CRE) to identify threats or security incidents that already occurred.
C. They detect if QRadar is operating at peak performance and error free.
D. They detect unusual traffic patterns in the network from the results of saved flow and events.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
To provide insight into why QRadar considers the event to be threatening, what does QRadar add to the Offense that users cannot edit or delete?
A. Source IP
B. Attack path
C. Annotations
D. Location
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
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. Source IP [Indexed]
B. Source or Destination IP
C. Any IP
D. Destination IP [Indexed]
Answer: (SHOW ANSWER)

NEW QUESTION: 34

Which considering the ability to tune False Positives with the Confidence factor Setting, which statement applies?
A. To ensure that the results are comparable, it is important to apply a common Confidence Factor across all network segments.
B. When setting a confidence factor, using a higher value will result in a higher number of Offenses.
C. Secure areas should have a lower confidence value, while less secure areas should have a higher confidence value.
D. Secure areas should have a higher confidence value, while less secure areas should have a lower confidence value a higher,,
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
What does the Assets tab provide?
A unified view of the information that is known about:
A. triggered Offenses.
B. events and flows.
C. log sources.
D. network devices.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
An analyst aims to improve the detection capabilities on all the Offense rules. QRadar SIEM has a tool that allows the analyst to update all the Building Blocks related to Host and Port Definition in a single page.
How is this accomplished?
A. Admin -> Asset Profile Configuration
B. Assets -> Server Discovery
C. Assets -> Asset Profiles
D. Admin -> Reference Set management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
How does an analyst view which rule triggered an Offense in the Offense summary page?
A. Display -> Rules
B. Actions -> Display Rules
C. Actions -> View Rules
D. Display -> Triggered Rules
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38

Where can an analyst working with Offenses add a regular expression test into an existing rule?
A. Top
B. Right
C. Left
D. Bottom
Answer: (SHOW ANSWER)

NEW QUESTION: 39
An analyst is working on Offense management and finds that a few of the offenses are not being removed from the Offense tab even after the Offense retention period has elapsed.
What could be the reason that these offenses are not being removed?
A. Offense has been annotated
B. Offense is inactive
C. Offense is released
D. Offense is protected
Answer: (SHOW ANSWER)
Explanation
https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-retention

NEW QUESTION: 40
What is the reason for this system notification?
"Time synchronization to primary or Console has failed"
A. Deny ntpdate communication on port 423.
B. Deny ntpdate communication on port 223.
C. Deny ntpdate communication on port 323.
D. Deny ntpdate communication on port 123
Answer: D (LEAVE A REPLY)
Explanation
https://www.ibm.com/docs/en/qradar-on-cloud?topic=appliances-time-synchronization-failed The managed host cannot synchronize with the console or the secondary HA appliance cannot synchronize with the primary appliance.
Administrators must allow ntpdate communication on port 123. When time synchronization is incorrect, data might not be reported correctly to the console. The longer the systems go without synchronization, the higher the risk that a search for data, report, or offense might return an incorrect result. Time synchronization is critical to successful requests from managed host and appliances

NEW QUESTION: 41
What information is displayed in the default "Log Activity" page? (Choose two.)
A. QID
B. Protocol

C. Qmap
D. Log Source
E. Event Name
Answer: (SHOW ANSWER)
Explanation
By default, the Log Activity tab displays the following parameters when you view normalized events:

Event Name	Specifies the normalized name of the event
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.

NEW QUESTION: 42
An analyst has been assigned a task to modify a rule in such a manner that Source IP of the triggered Offense from this rule should be stored in a Reference set.
Under which section of the rule wizard can the analyst achieve this?
A. Rule Response Limiter
B. Rule Test Stack Editor
C. Rule Response
D. Rule Action
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
An analyst wants to create a report using the report wizard.
What are key elements used by the wizard to create the report?
A. Report templates, layout, content.
B. Report templates, layout, saved searches
C. Layout, container, content
D. Report templates, user groups, permissions.
Answer: A (LEAVE A REPLY)