TestKing.C2150-195_104.Q&A

VCEplus.com

Number: C2150-195
Passing Score: 800
Time Limit: 120 min
File Version: 23.05

C2150-195

IBM Security QRadar V7.

- The answers of all questions are well modified.
- All the answers are appropriate and updated.
- Many new questions are added , Good for review go ahead and pass the exam now.
- I only used these questions and got 480 marks with this. Perfect Show.
- This is the best VCE I ever made. Try guys and if any suggestion please update this.

Exam A

QUESTION 1
An IBM Security QRadar V7.0 MR4 report can be generated into which three formats? (Choose three.)

A. XLS
B. PDF
C. CSV
D. DOC
E. JPEG
F. HTML

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
How would a user navigate to the Help menu in the IBM Security QRadar V7.0 MR4 (QRadar) interface?

A. Press Ctrl+H
B. Right-click on Item > Help
C. Help > QRadar Help Content
D. Select from the Action drop-down list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which statement about log source identifiers is true for the same log source identifier to be used more than once?

A. It must always be unique.
B. It must be unique amongst the same protocol.
C. It must be unique amongst the same log source group.

D. It must be unique amongst log sources of the same type

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
What is an Offense Type?

A. The offense response
B. A scoring priority of Set by Event
C. The destination of the e-mail notification sent
D. The index option chosen in the rule that created the offense

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
Which statement is most accurate regarding the information that NetFlow provides?

A. The start time of the conversation, the source and destination IP address, and the total bytes transferred.
B. The start time and the duration of the conversation, application ID, the source and the destination IP address.
C. The start time and duration of the conversation, the source and destination IP address, payload information, and the IP port number the data was sent to and received over.
D. The start time and duration of the conversation, the source and destination IP address, the IP port number the data was sent to and received over, and the total bytes transferred.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
How can a user quickly add a filter?

A. Actions > Add Filter
B. Click the Add Filter menu icon
C. Search > Edit Search, and add the filter
D. Right-click the column header > Add Filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 7
In the default Log Activity screen the right-click > False Positive menu is available in which column?

A. In every column
B. In every column header
C. In every column except time
D. In only the source and destination IP addresses columns

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
If an IBM Security QRadar V7.0 MR4 operator wants to detect a specific data string in the flow content, which search parameter should be used as a filter?

A. Source IP
B. Event Name
C. Remote Network
D. Source Payload Contains

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
What are two IT Security Frameworks? (Choose two.)

A. ITIL
B. SLA
C. COBIT
D. ISO 27001
E. Common Criteria

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
Which colored icon must be selected in the chart to change the chart type when viewing a grouped search?

A. The red X
B. The green star
C. The yellow gear
D. The blue question mark (?)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Where would a user set a searched view as the default view?

A. Under Save Criteria
B. Under the Admin tab
C. Select the View drop-down list
D. Select Default under the Actions menu

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
What effect does the Offense Retention period have on closed offenses and who can modify this period?

A. The Offense Retention period determines how long a closed offense will be kept in the database before it is deleted. The only person who can modify this period is an IBM Security QRadar V7.0 MR4 (QRadar) admin.
B. Once an offense is closed, any other QRadar user will be able to open it again for the time given by the Offense Retention period. The person who closes an offense is also the person who determines the offense retention period of the closed offense.
C. The offense retention period has no effect on closed offenses. A closed offense is the same as a deleted offense, and offenses that are deleted do not have a retention time. Only QRadar admins can change the offense retention period because it is found in the Admin tab.
D. The offense retention period has no effect on the closed offenses but only on offenses under evaluation. While the QRadar magistrate evaluates and correlates offenses, it may rely on the life span of an offense. Everyone who can create QRadar rules can modify the offense retention period.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
Which regex should be used to capture only the domain name blackbox.computerfor all future machine names based on this example?

`Computer=3 8 9.blackbox.computer'

A. Computer= (. *?) \s
B. Computer=389. (.*?)\s
C. Computer=(389\..*?)\s
D. Computer=. *?\. (.*?)\s

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
What must be done in order to save a search criteria as a quick search?

A. Select Save Criteria and select My Dashboard
B. Select Save Criteria in the New/Edit Search dialog
C. Right-click on the filter and select Save as Quick Search
D. Select Save Criteria and select Include in my Quick Searches

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
What are the three common fields on the Asset tab > VA Scan section? (Choose three.)

A. Potts
B. Status
C. Host Name
D. Asset Name
E. MAC Address
F. Next Run Time

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
For any Dashboard workspace, which two methods can be used to zoom into any of the spikes in traffic? (Choose two.)

A. Right-click on the peak of the spike
B. Double left-click on the peak of the spike
C. Hold the Shift key, left-click the mouse, drag to the right past the spike, and release the mouse button
D. Hold the Ctrl key. right-click the mouse, drag to the right past the spike, and release the mouse button
E. Hold the Shift key, right-click the mouse, drag to the right past the spike, and release the mouse button

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
How does IBM Security QRadar V7.0 MR4 (QRadar) use the information from vulnerability scanners?

A. The internal QRadar vulnerability scanner provides reports for auditors.
B. The results are used by QRadar to automatically patch and update the asset.
C. The information can be used to determine if an asset is vulnerable to an exploit.
D. Systems on which vulnerabilities are found are automatically monitored more closely.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
How can the time zone be changed for an existing report?

A. From the Report tab > Actions > select Time Zone
B. Right-click on the Report template > Change Time Zone
C. Select the report from the Reports tab > Options > Change Time Zone
D. Modify the template, under Chart Type select Define > select Time Zone

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Which search property is required for a user to create a Time Series chart?

A. Have a saved search filtered by an IP/CIDR
B. Have a saved search using an Order By option
C. Have a saved search displaying only two columns
D. Have a saved search with a Grouped By option enabled

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Which two components are only part of the IBM Security QRadar V7.0 MR4 (QRadar) SIEM and cannot be found in the QRadar Log Management? (Choose two.)

A. Console
B. Flow Collector
C. Event Collector
D. Event Processor
E. Offense Manager

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
Which search parameter in the Log Activity tab must be used to filter events by activity (e.g. SSH Login Succeeded)?

A. Category
B. Magnitude
C. User Name
D. Log Source

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is up-to-date.

QUESTION 22
What two tasks can be performed from the Assets tab? (Choose two.)

A. Edit asset severity
B. Clear vulnerabilities
C. Manually add asset profiles
D. Search assets that match specific attributes
E. Show which offenses an asset has been involved with

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Click the Exhibit button.

```
<13>Apr 17 00:23:40 user_desktop AgentDevice=WindowsLog
AgentLogFile=Security Source=Microsoft-Windows-Security-
Auditing Computer=389.blackbox.computer User= Domain=
EventID=5156 EventIDCode=5156 EventType=8
EventCategory=12810 RecordNumber=148983706
TimeGenerated=1334633018 TimeWritten=1334633018
Message=The Windows Filtering Platform has permitted a
connection. Application Information: Process ID: 1772 Application
Name: \device\harddiskvolume3\windows\system32\svchost.exe
Network Information: Direction: Inbound Source Address:
224.0.0.252 Source Port: 5355 Destination Address: 11.20.13.42
Destination Port: 61903 Protocol: 17 Filter Information: Filter Run-
Time ID: 66565 Layer Name: Receive/Accept Layer Run-Time ID:
44
```

What is the appropriate regex to extract the TirneWritten field value from the payload?

A. Written=.*\s
B. TimeWritten=.*\s
C. (TimeWritten=. *?\s)
D. TimeWritten=(. *?)\s

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Where would a user look to see the entire payload of an event?

A. The Raw Event tab
B. View > Show Payload
C. Right-click > Show Payload
D. The Payload Information section

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Which tab displays correlated security alerts in IBM Security QRadar V7.0 MR4?

A. Admin
B. Reports
C. Offenses
D. Log Activity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
How can a user quickly reload the default filter in their current tab?

A. Use the View option
B. Use the Display option
C. Clear all the current filters
D. Double-click the Tab button

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
How is an asset's weight used?

A. To classify the level of asset activity
B. To define the vulnerability of the asset
C. To determine how much emphasis IBM Security QRadar V7.0 MR4 gives when parsing logs
D. To determine the true severity and relevance of an event when the asset is involved in an offense

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
What is the main difference between a QFlow record versus a netflow capable router or switch?

A. QFlow can be used to trigger an alert.
B. QFlow cannot capture the communication payload.
C. QFlow can also be viewed in the Event Viewer window.
D. QFlow and vFlow can capture the communication payload.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
A user is complaining about slow traffic on a specific network segment, and an administrator has been asked to investigate the source of the congestion using an IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications.

From the Top Applications dashboard workspace, which tab is displayed when View Details is clicked?

A. Assets
B. Offenses
C. Log Activity
D. Network Activity

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 30
When working with rules, why do some rules specify QID values and some specify events?

A. Only low and high level categories can be specified within rules.
B. It is a matter of convention; QIDmap and event names are the same.
C. Event names are more precise; multiple events can be to the same QIDmap entry.
D. QID values are more precise; multiple QIDmap entries can be to same event name.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
How is the real time streaming of payloads for events viewed?

A. View drop-down > Raw Events
B. Action menu > View Raw Events
C. Display drop-down > Raw Events
D. Right-click on the events > View Raw Events

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
What action must be taken to view reports related to PCI specifically?

A. Right-click on Compliance and select PCI group.
B. There are no filtering or grouping capabilities for reports.

C. Click on the Group drop-down menu and select the category.
D. SSH to the Console and execute a GREP command to find PCI report options.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
What are three of the basic pre-built Dashboard Overview types? (Choose three.)

A. Administrator
B. Network Overview
C. Server Monitoring
D. System Monitoring
E. Application Performance
F. Threat and Security Monitoring

Correct Answer: BDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
What are three regulatory reports standard in IBM Security QRadar V7.0 MR4? (Choose three.)

A. SOX
B. NERC
C. HIPAA
D. BASEL
E. GPG13
F. ISO-9001

Correct Answer: ABC
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 35
How can a user clear all filters and return to the default search in the Log Activity user interface?

A. Search > Default Search
B. Action menu > Clear All Filters
C. Double-click the Log Activity tab
D. Right-click on the filter and select Clear Filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
When investigating an offense, how can a user gather information about the source IP address within IBM Security QRadarV7.0MR4?

A. Ping the IP address
B. Perform a NMap scan
C. Perform a Google search
D. Mouse over the source IP address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
In the Offense Summary page, which field indicates if an attack was sudden or if the attack occurred over a long period of time?

A. Duration
B. Total Time

C. Attack Length
D. Offense Period

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
corrected and valid.

QUESTION 38
What are two ways that asset profiles can be populated? (Choose two.)

A. Flow data
B. Heartbeat traffic
C. Router configuration
D. Windows application logs
E. Vulnerability assessment scans

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 39
Which four fields are used when importing assets from a CSV file?

A. IP, Name, Weight. Description
B. IP. Port, MAC Address, Weight
C. IP, Port. MAC Address. Description
D. IP, User, Host Name, Service Version

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
A flow is always based on what?

A. unicast and any cast traffic
B. unicast and broadcast traffic
C. unicast. multicast, and anycast traffic
D. unicast, broadcast, and multicast traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
Which two formats can a user export flow data from the Network Activity tab? (Choose two.)

A. RTF
B. XML
C. PDF
D. CSV
E. HTML

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
What is an example of a correctly written single character wild card search term using the Quick Filter?

A. Firewall
B. F(?)rewall
C. "F"(?)"rewall"
D. "FT ?)"rewall"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
How can a user cancel a running report in IBM Security QRadar V7.0 MR4?

A. A running report cannot be canceled
B. Select the report > Actions > Cancel Report
C. Right-click on the report > select Cancel Report
D. Look at the report queue, select the report to be canceled, select Delete

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
Which protocol can be used to send reports?

A. FTP
B. SMTP
C. SNMP
D. Syslog

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
If a user wants to assign an incident to a particular user, which drop-down list would they select inside the Offense interface?

A. Display

B. Actions
C. Incident
D. Question Mark

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
IBM Security QRadar V7.0 MR4 (QRadar) events that match a particular QRadar event rule are given a magnitude. This magnitude is a combination of which three factors?

A. Severity. Relevance, Weight
B. Severity, Frequency, Weight
C. Severity, Quantity, Credibility
D. Severity, Relevance, Credibility

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
Approximately how many default reports are included in IBM Security QRadar V7.0 MR4?

A. 100
B. 500
C. 1,000
D. 1,500

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 48
A flow is a sequence of packets that have which common characteristics?

A. Same source, MAC address, flow source and destination IP address
B. Same source IP address, flow source and transport layer port information
C. Same source and destination IP address and transport layer port information
D. Same destination IP address, source bytes and transport layer port information

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
By default how often is the information on the Dashboard refreshed?

A. Every 30 seconds
B. Every 60 seconds
C. Every 90 seconds
D. Every 120 seconds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
When using the Quick Filter feature in the Network Activity tab, which character must be used in front of special characters to indicate that the character is part of the search term?

A. +(plus)
B. -(minus)
C. \ (backslash)
D. ? (question mark)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
How can a user search to show only hosts with vulnerabilities?

A. Change the risk level to a value greater than five
B. From the Assets tab click on VA Scan and view results
C. From the Assets tab select Actions > Show Vulnerabilities
D. Check the Show Only Hosts with Vulnerabilities checkbox

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
What is required for a custom report to be generated?

A. A saved search
B. Administrative access
C. A custom report group
D. Access to the Custom Reporting module

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
What are vulnerability scanners?

A. It is a tool that is designed to search the network to find open services running.
B. It is an automated process that periodically checks computers for known vulnerabilities.
C. It is a tool to execute known attacks on applications and to check if these applications are vulnerable to these types of attacks.
D. It is a tool that scans a knowledge database for vulnerabilities that may apply to an IT environment as a result of the type of systems available.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
What are three types of time options available to search on from the View pull-down menu under Network Activity and Log Activity? (Choose three.)

A. Last Year
B. Real Time
C. Last Month
D. Date Range
E. Last Interval
F. Last 45 Minutes

Correct Answer: BEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
Which two fields are common in the Network Activity and Log Activities tabs? (Choose two.)

A. Source IP
B. Username
C. Application
D. Source Bytes
E. Destination Port

Correct Answer: AE

Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 56
Which high level category is used for IBM Security QRadar V7.0 MR4 internal monitoring?

A. Audit
B. Internal
C. Monitor
D. QRadar

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Where are QID values displayed?

A. In the Asset Properties of the asset
B. In the QID map menu of the Adrnin tab
C. In the detailed view of the Network Activity tab
D. In the Additional Information section of the event

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
A user is complaining of slow traffic on a specific network segment. An administrator is investigating the source of the congestion using the IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications. The administrator has drilled down into the details of a traffic spike and is now on the Details tab.

If the administrator double-clicks on the top application in the list, and then sorts by the Total Bytes column, what information is displayed regarding the source and destination IPs of the devices?

A. The devices causing the least traffic for all applications
B. The devices causing the most traffic for all applications
C. The devices causing the least traffic for the selected application
D. The devices causing the most traffic for the selected application

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
What are two instances when IBM Security QRadar V7.0 MR4 performs a magnitude re-evaluation for an offense? (Choose two.)

A. At scheduled intervals
B. When the offense is closed
C. When the offense is created
D. When each event or flow is added
E. When the offense is assigned to a user

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
Which function queries for offenses using specific criteria and displays those offenses that match the criteria?

A. Find
B. Search
C. Offense Lookup
D. Right-click > Navigate

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
What is the most likely issue with creating a custom property with a bad regex?

A. It slows down the reports when they are executed.
B. It slows down the searching in the Log Activity Viewer.
C. It slows down the event parsing when events are processed.
D. It slows down the dashboard charts while searching for the data

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
What are two examples of an exact search phrase for finding Firewall deny events using the Quick Filter? (Choose two.)

A. Firewall deny
B. Firewall*deny
C. Firewall.*deny
D. Firewall + deny
E. "Firewall" + "deny"

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Which option must be selected to view the results of previously run searches from the Log Activity tab?

A. Edit Search
B. New Search
C. Save Criteria
D. Manage Search Results

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
What are three data types provided by right-clicking IP address > More Options list > Information menu? (Choose three.)

A. Port Scan
B. DateyTime
C. DNS lookup
D. WHOIS lookup
E. Source Summary
F. Destination Summary

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
Which item in the IBM Security QRadar V7.0 MR4 interface provides a context sensitive help page which is available for any page, window, or section?

A. Help > Documentation
B. type Help in the Search field
C. Help drop-down list > Category
D. The question mark in the far right corner

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 66
What is the difference between a report and a search in IBM Security QRadar V7.0 MR4?

A. Reports are predefined while searches are customizable by the user.
B. They are the same; there is no difference between reports and searches.
C. A report is a document that represents the output of searches. Results of multiple searches can be integrated into a single report.
D. Searches can be created on any combination of domains like Offenses, Log Activity, or Network Activity. Reports can only be created on a single domain.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
modified.

QUESTION 67
What are three chart types included in the IBM Security QRadar V7.0 MR4 Dashboard? (Choose three.)

A. Pie
B. Bar
C. Line
D. Area
E. Time Series
F. Stacked Bar

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
If an IBM Security QRadar V7.0 MR4 operator wants to make the log data view/search available as a Dashboard item, what specifically must be done with the saved log search?

A. The search must be assigned to a Group.
B. The search must be saved as a Quick Search.
C. The search results must be exported as an XML document.
D. The search must be grouped around a parameter such as Source IP, Destination IP, etc.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
What is used to parse an event (log record) in IBM Security QRadar V7.0 MR4?

A. CRE
B. DSMs
C. Qidmaps
D. Protocols

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Using the regex * (RecordNumber) = (. *?)\s', which capture group should be used to capture the digits?

A. 0
B. 1
C. 2
D. 3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Which flow direction would a user specify in order to see flows that are solely related to traffic that originates from the internal networks to external networks?

A. L2L
B. R2L
C. L2R
D. R2R

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
What is the Identity Information section used for?

A. To show which rules match an event
B. To show which log source an event belongs to
C. To show the High/Low level category of an event
D. To show the user information relative to an event

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
Which column in the log activity displays the coalesced value?

A. Count
B. Raw Count
C. Event Count

D. Roll-up Count

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
When investigating an offense, what is the best option to gather information about the destination IP addresses within IBM Security QRadar V7.0 MR4?

A. Analyze the destination IP addresses and look for recent activity
B. Analyze the destination IP addresses and look for DHCP addresses
C. Analyze the destination IP addresses and look for low asset weights
D. Analyze the destination IP addresses and look for critical services to determine if they are local or remote

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
Everyone involved in a forensic analysis is now convinced that account management events involving promotion of accounts to AD administrator groups must be reported on daily. What is the most efficient method to accomplish this in IBM Security QRadar V7.0 MR4 (QRadar)?

A. Such a report requires additional parsing of events using extra custom properties and then including these properties in a manual report.
B. A new rule must be created which triggers an offense every time an account is assigned to an AD administrator group. By examining the event in detail it can be determined if this was really an offense or not.
C. The detailed search that the user has used to identify the relevant events must be saved first. Once it is saved, then it can be reused on demand, and it can also be used to build a custom report which can then be scheduled.
D. Automation or scripting is out of the question. The user has to repeat the analysis manually every time a similar incident occurs. The best the user can do is document the steps so that it is repeatable by anyone with access to the QRadar interface.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 76
An IBM Security GRadar V7.0 MR4 (QRadar) user has access to QRadar offenses. How do offenses appear in their My Offenses page?

A. Rules that have been created by the admin and that trigger an offense will also automatically put the triggered offense under their My Offenses page.
B. When the admin accesses the All Offenses option, they select Offenses and drag and drop them to their My Offenses page. Other QRadar users will no longer see the offenses that are put under their My Offenses page.
C. Anyone with access to the Offenses page will see all offenses. Under the My Offenses option, the person will see all offenses that have been assigned to them for further analysis and processing. These offenses are assigned from the All Offenses page by choosing the Assign option from the Action menu.
D. Rules that trigger an offense can also be configured in such way that the resulting offense is automatically assigned to the QRadar user who is notified of the offense by e-mail. The rule is configured to send an e-mail and if the e-mail address matches an e-mail addresse of any of the QRadar users then this offense is automatically added to the My Offenses page of this user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
How can a user display Raw events?

A. View drop-down > Raw Events
B. Action menu > View Raw Events
C. Display drop-down > Raw Events
D. Right-click on the events > View Raw Events

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is perfected.

QUESTION 78
A user is complaining of slow traffic on a specific network segment. An administrator is investigating the source of the congestion using the IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications. The administrator has drilled down into the details of a traffic spike and is

now on the Details tab.

What information is shown when double-clicking on the top application in the list?

A. A list of flows sorted by time for the selected application
B. A list of flows sorted by time for all of the top applications listed
C. A list of flows sorted by total byte count for the selected application
D. A list of flows sorted by total byte count for all of the top applications listed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Given the IBM Security Framework, IBM Security QRadar V7.0 MR4 fits into which two security domains? (Choose two.)

A. Data
B. People and Physical Security
C. Infrastructure, Network, or Endpoint
D. Applications and Application Security
E. IT Security/Compliance Analytics and Reporting

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
What are three time range options in the New/Edit search dialog box? (Choose three.)

A. Recent
B. Last Year
C. Real Time
D. Next Week
E. Last Month

F. Specific Interval

Correct Answer: ACF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
How can a user pause live streaming events?

A. Action menu > Pause
B. Select the Pause icon
C. Display drop-down > Pause
D. Right-click on Events > Pause

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Which two pages or tabs are added to the IBM Security QRadar V7.0 MR4 (QRadar) Log Management product after it has been upgraded to QRadar SIEM? (Choose two.)

A. Admin
B. Reports
C. Offenses
D. Dashboard
E. Network Activity

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
If a user wants to search for Windows user login failures, which high/low level category should be used?

A. Windows/Failures
B. Authentication/Failures
C. Windows/User Login Failures
D. Authentication/User Login Failure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
On the Offense Summary page, which filter is executed when the Flows icon or the link with the number of flows is clicked on?

A. A flow filter with all flows matching the source IP address
B. A flow filter with all flows matching the destination IP address
C. A flow filter with the Custom Rule Engine rule(s) for the last 24 hours
D. A flow filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
On the Offenses tab, which option displays offenses by access, exploit, or malware?

A. By Rules
B. By Category
C. By Definition
D. By Source IP

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
The remote directory field can be left blank for which protocol?

A. FTP
B. TFTP
C. SFTP
D. FTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
What does it mean if events are coming in as stored?

A. The events are not mapped to an existing QID map.
B. The events are being captured and parsed by a DSM.
C. The events are being captured but not being parsed by a DSM.
D. The events are being stored on disk and will be parsed by a DSM later.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
If a report author shares a report with another IBM Security QRadar V7 0 MR4 user, what type of report access is granted to the other user?

A. The other user can only access the report if they are an administrator.

B. The other user can use the original report as if it were created by that person.
C. The report output will be defined by the intersection of networkobjects and log sources of alluser with whom the report is shared.
D. The other user will not have any access to the original report definition but can do as they please with the report definition of the shared copy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
What is a QID identifier?

A. A mapping of a single device to a Q1 Labs unique identifier.
B. A mapping of a single event of an external device to a Q1 Labs unique identifier.
C. A mapping of multiple events of a single external device to a Q1 Labs unique identifier.
D. A mapping of a single event to multiple external devices to a Q1 Labs unique identifier.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
super valid.

QUESTION 90
Which event search group contains default PCI searches?

A. Compliance
B. System Monitoring
C. Network Monitoring and Management
D. Authentication, Identity, and User Activity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
What is the rule for using the Quick Filter to group terms using logical expressions such as AND, OR, and NOT?

A. The syntax is not case sensitive.
B. The syntax is case sensitive and the operators must be upper case to be recognized as logical expressions and not as search terms.
C. The syntax is case sensitive and the operators must be placed between square brackets to be recognized as logical expressions and not as search terms.
D. The syntax is case sensitive and the operators must be lower case and placed between square brackets to be recognized as logical expressions and not as search terms.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
How can a report be set up with restricted user access?

A. Click Reports > Restrict Users
B. Click on Manage Groups and add the user to the Restricted Reports group
C. Select the appropriate users on the Report Editing wizard to access the reports
D. Click Admin > Users, edit each user, and create lists of report filters users are allowed to see

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
How many default dashboards are included in IBM Security QRadar V7.0 MR4?

A. 1
B. 2
C. 5
D. 8

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
Which flow source is most often sampled?

A. vFlow
B. sFlow
C. QFlow
D. netflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
Which steps are required to see hidden offenses in IBM Security QRadar V7.0 MR4 (QRadar)?

A. Contact the QRadar administrator to select Hidden Offenses and then choose the Show option from the Action menu.
B. From the Offenses page, navigate to All Offenses and open the Search menu. Select Edit Search and in the Search Parameters section, uncheckthe box Exclude Hidden Offenses.
C. From the Offenses page, navigate to the Offenses by Category, and click on Show Inactive Categories to display all hidden offenses. Click Hide Inactive Categories to hide them again.
D. Hidden Offenses are no longer associated with Offenses so a custom report and a search should be created that uses a search parameter where Associated with Offense equals False. To create a custom report, navigate to Reports and from the Actions menu select Create.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
If the IBM Security QRadar V7.0 MR4 operator wants to graph the flow data in the Network Activity tab, which three chart types can be presented? (Choose three.)

A. Pie Chart
B. Bar Chart
C. Line Chart
D. Area Chart
E. Gant Chart
F. Time Series Chart

Correct Answer: ABF
Section: (none)
Explanation

Explanation/Reference:
answer is appropriate.

QUESTION 97
On the Offense summary page, which filter is executed when the Events icon or the link with the number of events is clicked?

A. An event filter with all events matching the source IP address
B. An event filter with all events matching the destination IP address
C. An event filter with the Custom Rule Engine rule(s) for the last 24 hours
D. An event filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
What is a prerequisite to create a report that contains at least one bar chart?

A. Have a color display and enable the JPanel
B. Have the role assigned to create (graphical) reports
C. Choose a search that has accumulated properties for the report
D. The search contained in the report must aggregate the results at least along one property

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
Using Quick Filter, what is a correct search term to find Blocked related activities in the payload?

A. Blocked
B. "payload includes Blocked"
C. payload includes "Blocked"
D. (payload includes) Blocked

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
How does a user search for events by high/low level category?

A. Actions menu > add a filter
B. Display drop-down > select categories
C. Add Filter icon > Category drop-down
D. View drop-down > select By Category drop-down

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 101
Offenses can be exported to which two file formats? (Choose two.)

A. RTF
B. XML
C. PDF
D. CSV
E. HTML

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
In the All Offenses dialog box, which column are the offenses sorted by default?

A. Start Date
B. Magnitude
C. Description
D. Offense Type

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
How does a user access the Extract a Custom Property section from a paused event screen in the Log Activity tab?

A. Actions menu > Extract Property
B. Double-click the event > Extract Property
C. Actions menu > Show All > Extract Custom Property
D. Right-click on the event > Properties > Extract Property

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 104
Why is coalescing important to a non-admin user?

A. It saves space on disk.
B. It saves events per second.
C. It makes it faster to parse the events.
D. It makes events easier to read in the Log Activity screen.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
corrected.