www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

Offense chaining is based on which field that is specified in the rule?

A. Rule action field
B. Offense response field
C. Rule response field
D. Offense index field

Answer: D

Explanation:

Offense chaining in IBM Security QRadar SIEM V7.5 is based on the offense index field specified in the rule. This means that if a rule is configured to use a specific field, such as the source IP address, as the offense index field, there will only be one offense for that specific source IP address while the offense is active. This mechanism is crucial for tracking and managing offenses efficiently within the system.

Question: 2

What QRadar application can help you ensure that IBM GRadar is optimally configured to detect threats accurately throughout the attack chain?

A. Rules Reviewer
B. Log Source Manager
C. QRadar Deployment Intelligence
D. Use Case Manager

Answer: D

Explanation:

The IBM QRadar Use Case Manager application assists in tuning QRadar to ensure it is optimally configured for accurate threat detection throughout the attack chain. This application provides guided tips to help administrators adjust configurations, making QRadar more effective in identifying and mitigating security threats. The QRadar Use Case Manager plays a significant role in maintaining

the effectiveness of the QRadar deployment.

Question: 3

How can an analyst search for all events that include the keyword "access"?

A. Go to the Network Activity tab and run a quick search with the "access" keyword.
B. Go to the Log Activity tab and run a quick search with the "access" keyword.
C. Go to the Offenses tab and run a quick search with the "access" keyword.
D. Go to the Log Activity tab and run this AOL: select * from events where eventname like 'access'.

Answer: B

Explanation:

In IBM Security QRadar SIEM V7.5, to search for all events containing a specific keyword such as "access", an analyst should navigate to the "Log Activity" tab. This section of the QRadar interface is dedicated to viewing and analyzing log data collected from various sources. By running a quick search with the "access" keyword in the Log Activity tab, the analyst can filter out events that contain this term in any part of the log data. This functionality is crucial for identifying specific activities or incidents within the vast amounts of log data QRadar processes, allowing analysts to quickly hone in on relevant information for further investigation or action.

Question: 4

What feature in QRadar uses existing asset profile data so administrators can define unknown server types and assign them to a server definition in building blocks and in the network hierarchy?

A. Server roles
B. Active servers
C. Server discovery
D. Server profiles

Answer: C

Explanation:

In IBM Security QRadar SIEM V7.5, the feature that utilizes existing asset profile data to define unknown server types and assign them to server definitions in building blocks and in the network hierarchy is known as "Server Discovery." This feature grants permission to discover servers, thereby enabling administrators to identify and classify various server types within their network infrastructure, enhancing the overall asset management and security posture.

Question: 5

QRadar analysts can download different types of content extensions from the IBM X-Force Exchange portal. Which two (2) types of content extensions are supported by QRadar?

A. Custom Functions
B. Events
C. Flows
D. FGroup
E. Offenses

Answer: A, E

Explanation:

QRadar supports different types of content extensions that can be downloaded from the IBM X-Force Exchange portal. Among the supported content extensions are "Custom Functions" and "Offenses." These extensions allow for enhanced functionality and customization within QRadar, providing users with the ability

to tailor the system to specific security needs and requirements.

Question: 6

What right-click menu option can an analyst use to find information about an IP or URL?

A. IBM Advanced Threat lookup
B. Watson Advisor AI IOC Lookup
C. QRadar Anomaly lookup
D. X-Force Exchange Lookup

Answer: D

Explanation:

To find information about an IP or URL within QRadar, analysts can use the right-click menu option "X-Force Exchange Lookup." This option is available when right-clicking an IP address or URL from the Offenses tab or event details windows, providing direct access to the X-Force Exchange interface for detailed threat intelligence and contextual information.

Question: 7

On the Offenses tab, which column explains the cause of the offense?

A. Description
B. Offense Type
C. Magnitude
D. IPs

Answer: B

Explanation:

On the Offenses tab within QRadar, the "Offense Type" column explains the cause of the offense. The offense type is determined by the rule that triggered the offense, and it dictates the kind of information displayed in the Offense Source Summary pane. This helps analysts understand the nature and origin of the offense, facilitating more effective investigation and response actions.

Question: 8

When using the Dynamic Search window on the Admin tab, which two (2) data sources are available?

A. ASSETS
B. PAYLOAD
C. OFFENSES
D. AOL QUERY
E. SAVED SEARCHES

Answer: AC

Explanation:

In the Dynamic Search window on the Admin tab of QRadar, the available data sources include "Assets" and "Offenses." These options allow administrators and analysts to construct queries based on asset information or offense data, enabling targeted searches and analyses tailored to specific security concerns within the organization.

Question: 9

How can adding indexed properties to QRadar improve the efficiency of searches?

A. By reducing the size of the data set required to find non-indexed search values
B. By increasing the size of the data set required to find non-indexed search values
C. By slowing down the search process
D. By reducing the number of indexed search values

Answer: A

Explanation:

Adding indexed properties to QRadar can significantly improve the efficiency of searches by reducing the size of the data set required to locate matches for non-indexed search values. Indexing creates references to unique terms in the data and their locations, which means that the search engine can filter the data set by indexed properties first, eliminating irrelevant portions of the data set and thereby reducing the overall volume of data that needs to be searched.

Question: 10

Which type of rule should you use to test events or (lows for activities that are greater than or less than a specified range?

A. Behavioral rules
B. Anomaly rules
C. Custom rules
D. Threshold rules

Answer: D

Explanation:

Threshold rules in QRadar are designed to test events or flows for activities that are greater than or less than a specified range. These rules are particularly useful for detecting significant changes such as bandwidth usage variations, failed services, changes in the number of connected users, and large outbound data transfers. By setting acceptable limits within threshold rules, administrators can effectively monitor for and respond to abnormal activities within the network.

Question: 11

Which parameters are used to calculate the magnitude rating of an offense?

A. Relevance, credibility, time
B. Severity, relevance, credibility
C. Relevance, urgency, credibility
D. Severity, impact, urgency

Answer: B

Explanation:

The magnitude rating of an offense in IBM Security QRadar SIEM V7.5 is calculated based on three key parameters: severity, relevance, and credibility. Severity indicates the level of threat, relevance determines the offense's impact on the network, and credibility reflects the integrity of the offense as determined by the credibility rating configured in the log source. This combination of factors helps prioritize offenses and guide analysts on which ones to investigate first.

Question: 12

Reports can be generated by using which file formats in QRadar?

A. PDF, HTML, XML, XLS
B. JPG, GIF, BMP, TIF
C. TXT, PNG, DOC, XML
D. CSV, XLSX, DOCX, PDF

Answer: A

Explanation:

QRadar supports generating reports in various file formats, including PDF, HTML, XML, and XLS. These formats provide flexibility in how reports are viewed and shared, catering to different needs and preferences for report presentation and analysis.

Question: 13

The Use Case Manager app has an option to see MITRE heat map.

Which two (2) factors are responsible for the different colors in MITRE heat map?

A. Number of offenses generated
B. Number of events associated to offense
C. Number of rules mapped
D. Level of mapping confidence
E. Number of log sources associated

Answer: C, D

Explanation:

www.atmicnetworks.com

The MITRE heat map in the Use Case Manager app within QRadar uses several factors to determine the colors displayed, among which the number of rules mapped to MITRE ATT&CK tactics and techniques and the level of mapping confidence are crucial. These factors help visualize the coverage and reliability of rule mappings against the comprehensive MITRE ATT&CK framework, aiding in the identification of potential gaps or areas for improvement in threat detection capabilities.

Question: 14

In QRadar. what do event rules test against?

A. The parameters of an offense to trigger more responses
B. Incoming log source data that is processed in real time by the QRadar Event Processor
C. Incoming flow data that is processed by the QRadar Flow Processor
D. Event and flow data

Answer: B

Explanation:

Event rules in QRadar test against incoming log source data processed in real time by the QRadar Event Processor. This real-time processing enables QRadar to analyze and respond to security events as they occur, enhancing the system's ability to detect and mitigate threats promptly.

Question: 15

What two (2) guidelines should you follow when you define your network hierarchy?

A. Do not configure a network group with more than 15 objects.
B. Organize your systems and networks by role or similar traffic patterns.
C. Use the autoupdates feature to automatically populate the network hierarchy.
D. Import scan results into QRadar.
E. Use flow data to build the asset database.

Answer: B, E

Explanation:

When defining the network hierarchy in QRadar, it is recommended to organize systems and networks by role or similar traffic patterns to differentiate network behavior effectively. Additionally, it is advised not to configure a network group with more than 15 objects to avoid difficulties in viewing detailed information for each object and to ensure efficient management of network groups.

Question: 16

Create a list that stores Username as the first key. Source IP as the second key with an assigned cidr data type, and Source Port as the value.
The example above refers to what kind of reference data collections?

A. Reference map of sets
B. Reference store

C. Reference table
D. Reference map

Answer: C

Explanation:

The example provided refers to a "Reference table," which is a type of reference data collection in QRadar that can store complex structured data. A reference table allows for multiple keys and values, supporting the storage of data like Usernames, Source IPs with a specific data type (e.g., cidr for IP addresses), and Source Ports as values.

Question: 17

What type of custom property should be used when an analyst wants to combine extraction-based URLs, virus names, and secondary user names into a single property?

A. AOL-based property
B. Absolution-based property
C. Extraction-based property
D. Calculation-based property

Answer: A

Explanation:

When an analyst wants to combine multiple extraction and calculation-based properties into a single property, such as URLs, virus names, and secondary user names, an AQL-based property should be used. AQL (Ariel Query Language)-based properties allow for the aggregation of diverse data types into a unified custom property, facilitating more flexible and comprehensive data analysis within QRadar.

Question: 18

What happens when you select "False Positive" from the right-click menu in the Log Activity tab?

A. You can tune out events that are known to be false positives.

B. You can investigate an IP address or a user name.
C. Items are filtered that match or do not match the selection.
D. The selected event is filtered based on the selected parameter in the event.

Answer: A

Explanation:

Selecting "False Positive" from the right-click menu in the Log Activity tab opens a window that enables users to tune out events that are known to be false positives, preventing them from generating offenses. This feature is crucial for minimizing noise and focusing on genuine threats, thereby enhancing the efficiency of threat detection and response processes within QRadar.

Question: 19

Which statement regarding saved event search criteria is true?

A. Saved search criteria expires
B. Saved search criteria does not expire
C. Saved search criteria cannot be reused
D. You cannot define the name of the saved search criteria

Answer: B

Explanation:

In QRadar, when you save search criteria, especially on the Offenses tab, the configured search criteria are retained for future use and do not expire. This permanence ensures that users can quickly access and reuse their preferred search configurations, thereby streamlining the process of monitoring and investigating offenses over time.

Question: 20

Which two (2) aggregation types ate available for the pie chart in the Pulse app?

A. Last
B. Total
C. Average
D. First
E. Middle

Answer: B, C

Explanation:

For pie charts in the Pulse app of QRadar, the available aggregation types include "Total" and "Average." These aggregation types allow for the representation of data in a manner that summarizes the total sum of the data points or their average value, respectively, providing insightful and concise visualizations of the data within the Pulse app dashboards. This information is implied from the general capabilities of dashboard items in QRadar, as detailed in the provided

documentation, which typically includes such aggregation options for data visualization.

Question: 21

A QRadar analyst wants to limit the time period for which an AOL query is evaluated. Which functions and clauses could be used for this?

A. START, BETWEEN. LAST. NOW. PARSEDATETIME
B. START, STOP. LAST, NOW, PARSEDATETIME
C. START. STOP. BETWEEN, FIRST
D. START, STOP. BETWEEN, LAST

Answer: B

Explanation:

In QRadar, to limit the time period for which an AQL (Ariel Query Language) query is evaluated, the functions and clauses that can be used include START, STOP, LAST, NOW, and PARSEDATETIME.
Specifically, the LAST function is used to define a relative time range for the query, such as "LAST 2 DAYS".

Question: 22

Which of these statements regarding the deletion of a generated content report is true?

A. Only specific reports that were not generated from the report template as well as the report template are deleted.
B. All reports that were generated from the report template are deleted, but the report template is retained.
C. All reports that were generated from the report template as well as the report template are deleted.
D. Only specific reports that were not generated from the report template are deleted, but the report template is retained.

Answer: B

Explanation:

When deleting a generated content report in QRadar, all reports that were generated from the report template are deleted, but the report template itself is retained. This ensures that the structure for generating future reports remains intact, while only the instances of reports generated from that template are removed.

Question: 23

The Pulse app contains which two (2) widget chart types?

A. Small number chart
B. Hexadecimal chart
C. Binary chart
D. Scatter chart
E. Big number chart

Answer: D, E

Explanation:

Widget chart types - IBM Documentation

Question: 24

Which two (2) values are valid for the Offense Type field when a search is performed in the My Offenses or All Offenses tabs?

A. QID
B. Any
C. Risk Score
D. DDoS
E. Source IP

Answer: BE

Explanation:

In QRadar, when performing a search in the My Offenses or All Offenses tabs, valid values for the Offense Type field include "Any" and "Source IP". "Any" searches all offense sources, while "Source IP" allows for searching offenses with a specific source IP address.

Question: 25

How long does QRadar store payload indexes by default?

A. 7 days
B. 30 days
C. 14 days
D. 90 days

Answer: B

Explanation:

By default, QRadar stores payload indexes for a duration of 30 days. This retention period is configurable, allowing administrators to adjust how long specific data is retained based on their requirements.

Question: 26

On the Reports tab in QRadar. what does the message "Queued (position in the queue)" indicate

when generating a report?

A. The report is scheduled to run, and the message is a count-down timer that specifies when the report will run next.
B. The report is ready to be viewed in the Generated Reports column.
C. The report is generating.
D. The report is queued for generation and the message indicates the position of the report in the queue.

Answer: D

Explanation:

In the Reports tab of QRadar, the message "Queued (position in the queue)" indicates that the report is queued for generation. The message provides the position of the report within the generation queue, which helps users understand the report's status and expected generation time

Question: 27

What does an analyst need to do before configuring the QRadar Use Case Manager app?

A. Create a privileged user.
B. Run a QRadar health check.
C. Check the license agreement.
D. Create an authorized service token.

Answer: D

Explanation:

Before configuring the QRadar Use Case Manager app, it is essential to ensure that the app has the necessary permissions to function correctly. This typically involves creating an authorized service token which provides the app with the permissions to access and manage the QRadar environment.

Question: 28

Which two (2) options are at the top level when an analyst right-clicks on the Source IP or Destination IP that is associated with an offense at the Offense Summary?

A. Information
B. DNS Lookup
C. Navigate
D. WHOIS Lookup
E. Asset Summary page

Answer: B, D

Explanation:

When an analyst right-clicks on the Source IP or Destination IP that is associated with an offense at the Offense Summary in QRadar, two of the top-level options are DNS Lookup and WHOIS Lookup1. These options provide additional information about the IP address, such as its domain name (DNS Lookup) and registration information (WHOIS Lookup)1.

Question: 29

When searching for all events related to "Login Failure", which parameter should a security analyst use to filter the events?

A. Event Asset Name
B. Event Collector
C. Anomaly Detection Event
D. Event Name

Answer: D

Explanation:

When searching for all events related to "Login Failure," a security analyst should use the Event Name parameter to filter the events. This allows the analyst to specifically target events with descriptions such as "Database Login Failure," which indicates that a database login attempt failed.

Question: 30

Which two (2) options are used to search offense data on the By Networks page?

A. Raw/Flows
B. Events/Flows
C. NetIP
D. Severity
E. Network

Answer: BE

Explanation:

To search offense data on the By Networks page, an analyst can use the options "Events/Flows" to filter based on the types of data points, and "Network" to specify the network they want to search for. This allows for a focused search on specific networks and types of data.

Question: 31

After how much time will QRadar mark an Event offense dormant if no new events or flows occur?

A. 2 hours
B. 30 minutes
C. 24 hours
D. 5 minutes

Answer: B

Explanation:

QRadar will mark an Event offense as dormant if no new events or flows occur within 30 minutes. However, if QRadar did not process any events within 4 hours, this also triggers the offense to become dormant. Once dormant, the offense remains in this state for 5 days unless new events or flows are added.

Question: 32

What Is the result of the following AQL statement?

SELECT * FROM events WHERE username ILIKE '-.EF.SS'

A. Returns all fields where the username contains the ERS string and is case-sensitive
B. Returns all fields where the username contains the ERS string and is case-insensitive
C. Returns all fields where the username is different from the ERS string and is case-insensitive

D. Returns all fields where the username is different from the ERS string and is case-sensitive

Answer: B

Explanation:

The AQL (Ariel Query Language) statement provided would return all fields from the 'events' table where the 'username' column contains the string 'ERS', regardless of case. The 'ILIKE' operator in AQL is used for case-insensitive pattern matching, which means that it will match 'ers', 'Ers', 'ErS', etc.

Question: 33

Which two (2) types of data can be displayed by default in the Application Overview dashboard?

A. Login Failures by User {real-time)
B. Flow Rate (Flows per Second - Peak 1 Min)
C. Top Applications (Total Bytes)
D. Outbound Traffic by Country (Total Bytes)
E. ICMP Type/Code (Total Packets)

Answer: C, D

Explanation:

The Application Overview dashboard in QRadar includes various default items1. Two of these items are Top Applications (Total Bytes) and Outbound Traffic by Country (Total Bytes)1.
Default dashboards - IBM Documentation
According to the IBM Security QRadar SIEM V7.5 documentation, the Application Overview dashboard by default includes items such as "Inbound Traffic by Country (Total Bytes)," "Outbound Traffic by Country (Total Bytes)," and "Top Applications (Total Bytes)" among others. This confirms that options C and D are displayed by default on the Application Overview dashboard.

Question: 34

What process is used to perform an IP address X-Force Exchange Lookup in QRadar?

A. Offense summary tab > right-click IP address > Plugin Option > X-Force Exchange Lookup
B. Copy the IP address and go to X-Force Exchange to perform the lookup
C. Run Autoupdate
D. Run a query on maxmind db

Answer: A

Explanation:

To perform an IP address X-Force Exchange Lookup in QRadar, you can follow these steps2:
Select the Log Activity or the Network Activity tab.
Right-click the IP address that you want to view in X-Force Exchange.
Select More Options > Plugin Options > X-Force Exchange Lookup to open the X-Force Exchange interface2.
The procedure to perform an IP address X-Force Exchange Lookup in QRadar involves selecting either the Log

Activity or the Network Activity tab, right-clicking the IP address of interest, and then navigating through More Options > Plugin Options > X-Force Exchange Lookup to access the X-Force Exchange interface.

Question: 35

The magnitude rating of an offense in QRadar is calculated based on which values?

A. Relevance, severity, importance
B. Relevance, credibility, severity
C. Criticality, severity, importance
D. Criticality, severity, credibility

Answer: B

Explanation:

The magnitude rating of an offense in QRadar is calculated based on relevance, severity, and credibility. Relevance determines the impact on the network, credibility indicates the integrity of the offense, and severity represents the level of threat. QRadar uses complex algorithms to calculate and periodically re-evaluate the offense magnitude rating.

Question: 36

DRAG DROP
Select all that apply

What is the sequence to create and save a new search called "Offense Data" that shows all the CRE events that are associated with offenses?

www.atmicnetworks.com

Unordered Options

From the QRadar Console, click Save Criteria

Click Search.

Under Search Parameters, add Associated with Offense Is True and Log Source Type is Custom Rule Engine

From the QRadar Console, click the Log Activity tab. Click Search > New Search.

Provide the Search Name "Offense Data" and click OK.

Ordered Options

Explanation:

Answer

Ordered Options

1 From the QRadar Console, click Save

2 From the QRadar Console, click the Li Search > ivity tab. Click New Search.

3 Provide the Search Name 'Offense Data" and click OK.

4 Under Search Parameters, add Associated with Offense is True and Log Source Type is Custom Rule Engine.

5 Click Search.

Question: 37

A QRadar analyst develops an advanced search on the Log Activity tab and presses the shortcut "Ctrl + Space" in the search field. What information is displayed?

A. The full list of AQL databases, functions and fields (properties) is displayed.
B. The full list of AQL tables and relationships from a database is displayed.
C. The full list of AOL functions, fields (properties), and keywords is displayed.
D. The full list of AQL functions, tables, and views from a database is displayed.

Answer: A

Explanation:

The information displayed when pressing "Ctrl + Space" in the search field in the Log Activity tab in QRadar is not explicitly mentioned in the search results. However, in general, this shortcut is often used in various software and platforms to display a list of available commands, functions, or properties. In the context of QRadar, it's likely that pressing "Ctrl + Space" in the search field would display a list of available AQL (Ariel Query Language) databases, functions, and fields (properties).

Question: 38

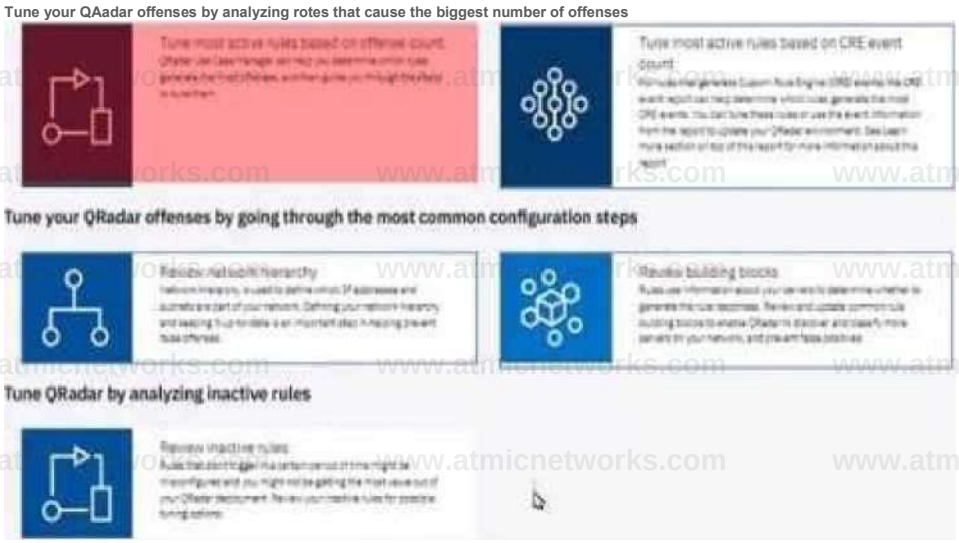
HOTSPOT

New vulnerability scanners are deployed in the company's infrastructure and generate a high

number of offenses. Which function in the Use Case Manager app does an analyst use to update the list of vulnerability scanners?

Answer:

Explanation:



Question: 39

Which two (2) types of categories comprise events?

A. Unsupported
B. Unfound
C. Stored
D. Found
E. Parsed

Answer: C, E

Explanation:

While the documentation does not explicitly list "Stored" and "Parsed" as categories comprising events, it discusses high-level event categories and the process of categorizing incoming events for easy searching.

Without specific mention of the categories "Stored" and "Parsed," the provided documentation does not verify any of the options directly. Further insight into event categories is provided by discussing how events are grouped into high-level categories for organizational purposes.

Question: 40

AQRadar analyst can check the rule coverage of MITRE ATT&CK tactics and techniques by using Use Case Manager.

In the Use Case Manager app, how can a QRadar analyst check the offenses triggered and mapped to MITRE ATT&CK framework?

A. By navigating to "CRE Report"
B. From Offenses tab
C. By clicking on "Tuning Home"
D. By navigating to "Detected in timeframe"

Answer: D

Explanation:

To check the offenses triggered and mapped to the MITRE ATT&CK framework using the Use Case Manager app, an analyst can navigate through the Offenses tab, click on All Offenses, and then utilize the All Offenses Summary toolbar to display rules contributing to an offense. This process allows for an investigation into how offenses correlate with the MITRE ATT&CK framework. However, the exact option "Detected in timeframe" is not explicitly mentioned in the provided documentation, and the described procedure offers a broader approach to reviewing offenses and their associated rules within the MITRE ATT&CK context.

Question: 41

Events can be exported from the QRadar Log Activity tab in which file formats?

A. JSON. XML, and CSV
B. XLS and CSV
C. JSON and XML
D. XML and CSV

Answer: D

Explanation:

Events can be exported from the QRadar Log Activity tab in XML (Extensible Markup Language) or CSV (Comma-Separated Values) formats, providing flexibility in how data is extracted and used for further analysis outside of QRadar.

Question: 42

In Rule Response, which two (2) options are available for Offense Naming?

A. This information should be removed from the current name of the associated offenses
B. This information should contribute to (he name of the associated offenses

C. This information should set or replace the name of the associated offenses
D. This information should contribute to the dispatched event name of the associated offenses.
E. This information should contribute to the category naming of the associated offenses

Answer: BC

Explanation:

In Rule Response for Offense Naming, QRadar provides options to either contribute to or set/replace the name of the associated offenses. These options allow for dynamic naming of offenses based on event name information, facilitating easier identification and categorization of offenses.

Question: 43

A task is set up to identify events that were missed by the Custom Rule Engine. Which two (2) types of events does an analyst look for?

A. Log Only Events sent to a Data Store
B. High Level Category: User Defined Events
C. Forwarded Events to different destination
D. High Level Category Unknown Events
E. Low Level Category: Stored Events

Answer: A, D

Explanation:

To identify events that were missed by the Custom Rule Engine (CRE) in IBM Security QRadar SIEM, an analyst would primarily look for "Log Only Events sent to a Data Store" and "High Level Category Unknown Events." Log Only Events are those that are stored directly without being processed by the CRE, indicating they might have been overlooked or not matched by any existing rules. High Level Category Unknown Events are those that do not fit into any of the predefined categories in QRadar, suggesting that the CRE might not have rules to handle or categorize these events properly. These types of events are crucial for analysts to review to ensure that no significant incidents are missed and to refine the rule set for better detection in the future.

Question: 44

When examining lime fields on Event Information, which one represents the time QRadar received the raw event?

A. Processing Time
B. Log Source Time
C. Start Time
D. Storage Time

Answer: C

Explanation:

The "Start Time" timestamp represents when an event is received by a QRadar Event Collector, marking the moment QRadar first becomes aware of the event. This is crucial for understanding the timing of event

www.atmicnetworks.com

processing and potential delays in the event pipeline.

Question: 45

What is the default number of notifications that the System Notification dashboard can display?

A. 50 notifications
B. 20 notifications
C. 10 notifications
D. 5 notifications

Answer: C

Explanation:

The default setting for the System Notification dashboard is to display 10 notifications, providing a manageable overview of system alerts and issues. Users can adjust this setting to view fewer or more notifications based on their preferences.

Question: 46

What does this example of a YARA rule represent?

A. Flags containing hex sequence and str1 less than three times
B. Flags content that contains the hex sequence, and hex! at least three times
C. Flags for str1 at an offset of 25 bytes into the file
D. Flags content that contains the hex sequence, and str1 greater than three times

Answer: C

Explanation:

A YARA rule is used for malware identification and classification, based on textual or binary patterns. The example provided suggests a rule that flags occurrences of a specific string (str1) at a precise location within a file. The "offset" keyword in YARA rules specifies the exact byte position where the pattern (in this case, 'str1') should appear. Thus, the correct interpretation of the YARA rule example is that it flags instances where 'str1' appears 25 bytes into the file, indicating a very specific pattern match used for identifying potentially malicious files or activities that conform to this pattern.

Question: 47

On which lab can an analyst perform a "Flow Bias" Quick Search?

A. Asset Management app
B. Log Activity tab
C. Log Source Management app
D. Network Activity tab

Answer: D

Explanation:

A "Flow Bias" Quick Search can be performed from the Network Activity tab in QRadar, providing insights into network flows and potential anomalies or biases in the traffic patterns.

Question: 48

Which reference set data element attribute governs who can view its value?

A. Tenant Assignment
B. Origin
C. Reference Set Management MSSP
D. Domain

Answer: D

Explanation:

The Domain attribute governs who can view the value of a reference set data element, ensuring that only users with appropriate domain access or tenant assignments can view the data. This is essential for maintaining data visibility and access control within a multi-tenant QRadar environment.

Question: 49

Which two (2) components are necessary for generating a report using the QRadar Report wizard?

A. Saved search
B. Dynamic search
C. Layout
D. Quick search
E. Email address

Answer: AC

Explanation:

In IBM Security QRadar SIEM, generating a report using the QRadar Report Wizard requires a "Saved Search" and a "Layout." A Saved Search is a predefined search criterion that users save in QRadar to reuse for various reporting or analysis purposes. It acts as the data source for the report, defining what data will be included. The Layout component refers to the structure and presentation of the report, including how the data from the Saved Search is organized and displayed. It encompasses the

formatting, charts, tables, and other visual elements that make up the final report. Together, these components ensure that reports are not only informative but also well-organized and readable, catering to the specific informational needs and preferences of the users or stakeholders.

Question: 50

What are two characteristics of a SIEM? (Choose two.)

A. Log Management

B. System Deployment
C. Endpoint Software patching
D. Enterprise User management
E. Event Normalization & Correlation

Answer: A, E

Explanation:

Question: 51

Which QRadar component provides the user interface that delivers real-time flow views?

A. QRadar Viewer
B. QRadar Console
C. QRadar Flow Collector
D. QRadar Flow Processor

Answer: B

Explanation:

Reference:
http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/shc_qradar comps.html

Question: 52

Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC
B. McAfee ePolicy Orchestrator via JDBC
C. McAfee ePolicy Orchestrator via SNMP
D. Solaris Basic Security Mode (BSM) via Log File Protocol

Answer: C

Explanation:

Question: 53

A mapping of a username to a user's manager can be stored in a Reference Table and output in a search or a report.
Which mechanism could be used to do this?

A. Quick Search filters can select users based on their manager's name.
B. Reference Table lookup values can be accessed in an advanced search.
C. Reference Table lookup values can be accessed as custom event properties.
D. Reference Table lookup values are automatically used whenever a saved search is run.

Answer: B

Explanation:

Question: 54

Which kind of information do log sources provide?

A. User login actions
B. Operating system updates
C. Flows generated by users
D. Router configuration exports.

Answer: A

Explanation:

Question: 55

How does a Device Support Module (DSM) function?

A. A DSM is a configuration file that combines received events from multiple log sources and displays them as offenses in QRadar.
B. A DSM is a background service running on the QRadar appliance that reaches out to devices deployed in a network for configuration data.
C. A DSM is a configuration file that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.
D. A DSM is an installed appliance that parses received events from multiple log sources and converts them to a standard taxonomy format that can be displayed as outputs.

Answer: D

Explanation:

Question: 56

Which flow fields should be used to determine how long a session has been active on a network?

A. Start time and end time
B. Start time and storage time
C. Start time and last packet time
D. Last packet time and storage time

Answer: C

Explanation:

Question: 57

Which browser is officially supported for QRadar?

A. Safari version 9.0-3
B. Chromium version 33
C. 32-bit Internet Explorer 9
D. Firefox version 38.0 ESR

Answer: C

Explanation:

Question: 58

A Security Analyst was asked to search for an offense on a specific day. The requester was not sore of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username. Which fitters can the Security Analyst use to search for the information requested?

A. Offense ID, Source IP, Username
B. Magnitude, Source IP, Destination IP
C. Description, Destination IP. Host Name
D. Specific Interval, Username, Destination IP

Answer: D

Explanation:

Question: 59

What is an effective method to fix an event that is parsed an determined to be unknown or in the wrong QReader category/

A. Create a DSM extension to extract the category from the payload
B. Create a Custom Property to extract the proper Category from the payload
C. Open the event details, select map event, and assign it to the correct category
D. Write a Custom Rule, and use Rule Response to send a new event in the proper category

Answer: B

Explanation:

Question: 60

Which type of rule requires a saved search that must be grouped around a common parameter

A. Flow Rule
B. Event Rule
C. Common Rule
D. Anomaly Rule

Answer: B

Explanation:

www.atmicnetworks.com

Question: 61

What can be considered a log source type?

A. ICMP
B. SNMP
C. Juniper IOP
D. Microsoft SMBtail

Answer: C

Explanation:

Question: 62

Which two high level Event Categories are used by QRadar? (Choose two.)

A. Policy
B. Direction
C. Localization
D. Justification
E. Authentication

Answer: A, E

Explanation:

Question: 63

A Security Analyst has noticed that an offense has been marked inactive.
How long had the offense been open since it had last been updated with new events or flows?

A. 1 day + 30 minutes
B. 5 days + 30 minutes
C. 10 days + 30 minutes
D. 30 days + 30 minutes

Answer: B

Explanation:

Question: 64

What is the effect of toggling the Global/Local option to Global in a Custom Rule?

A. It allows a rule to compare events & flows in real time.
B. It allows a rule to analyze the geographic location of the event source.
C. It allows rules to be tracked by the central processor for detection by any Event Processor.

www.atmicnetworks.com

D. It allows a rule to inject new events back into the pipeline to affect and update other incoming events.

Answer: D

Explanation: