IBM.C1000-162.by.Tom.38q

Number: C1000-162
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: C1000-162

Exam Name: IBM Certified Analyst - Security QRadar SIEM V7.5

Exam A

QUESTION 1
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.

Correct Answer: B
Section:
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 2
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

Correct Answer: C
Section:
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 processing and potential delays in the event pipeline.

QUESTION 3
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

Correct Answer: D
Section:

QUESTION 4
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

Correct Answer: B
Section:

QUESTION 5
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

Correct Answer: B
Section:

QUESTION 6
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

Correct Answer: D
Section:
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 7
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'.

Correct Answer: B
Section:
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 8
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

Correct Answer: C
Section:

QUESTION 9
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.

Correct Answer: B
Section:

QUESTION 10
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.

Correct Answer: A
Section:

QUESTION 11
On the Offenses tab, which column explains the cause of the offense?

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

Correct Answer: B
Section:
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 12
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

Correct Answer: A, C
Section:
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 13
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

Correct Answer: A
Section:
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 14
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

Correct Answer: D
Section:
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 15
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

Correct Answer: B
Section:
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 16
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

Correct Answer: A
Section:
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.

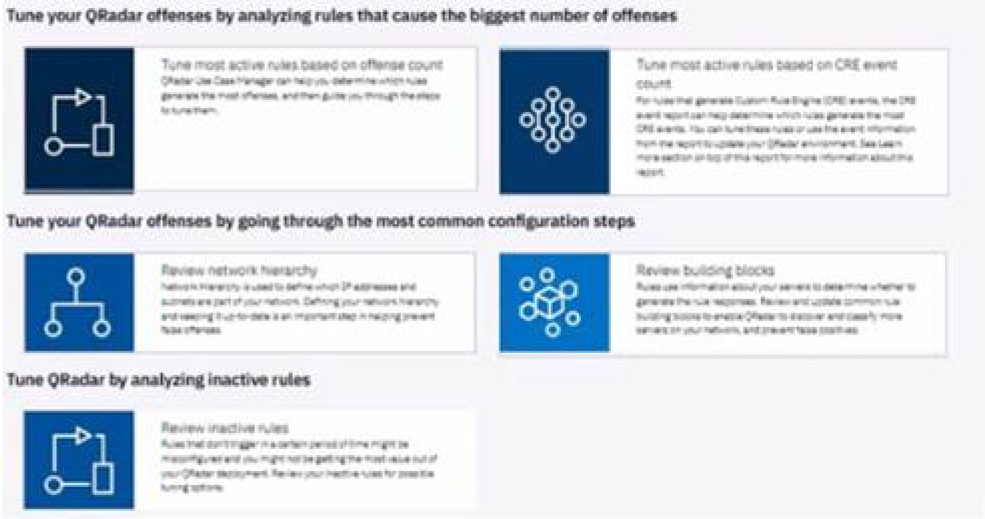
QUESTION 17
A QRadar analyst develops an advanced search on the Log Activity tab and presses the shortcut 'Ctrl + Space' in the search field. What information is displayed?

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.

Correct Answer: A
Section:
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 18
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?

Hot Area:



Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses

Tune most active rules based on offense count
QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.

Tune most active rules based on CRE event count
For rules that generate Custom Rule Engine (CRE) events, the CRE event report can help determine which rules generate the most CRE events. You can tune these rules or use the event information from the report to update your QRadar environment. See Learn more section on top of this report for more information about this report.

Tune your QRadar offenses by going through the most common configuration steps

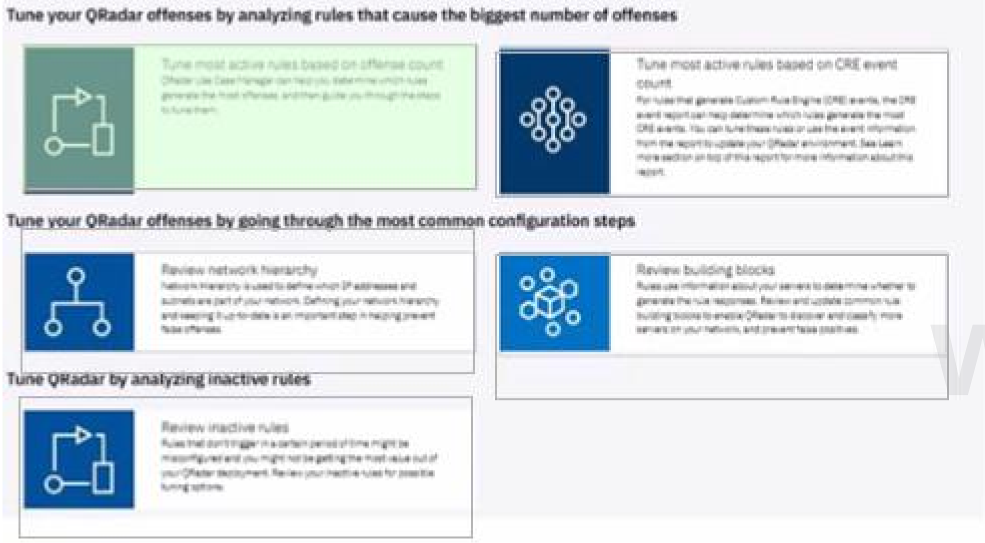
Review network hierarchy
Network hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.

Review building blocks
Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.

Tune QRadar by analyzing inactive rules

Review inactive rules
Rules that don't trigger in a certain period of time might be misconfigured and you might not be getting the most value out of your QRadar deployment. Review your inactive rules for possible tuning options.

Answer Area:



Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses

Tune most active rules based on offense count
QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.

Tune most active rules based on CRE event count
For rules that generate Custom Rule Engine (CRE) events, the CRE event report can help determine which rules generate the most CRE events. You can tune these rules or use the event information from the report to update your QRadar environment. See Learn more section on top of this report for more information about this report.

Tune your QRadar offenses by going through the most common configuration steps

Review network hierarchy
Network hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.

Review building blocks
Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.

Tune QRadar by analyzing inactive rules

Review inactive rules
Rules that don't trigger in a certain period of time might be misconfigured and you might not be getting the most value out of your QRadar deployment. Review your inactive rules for possible tuning options.

Section:
Explanation:

QUESTION 19

Which two (2) types of categories comprise events?

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

Correct Answer: C, E
Section:
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 20

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'

Correct Answer: D
Section:
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 21

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

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

Correct Answer: D
Section:
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 22

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

Correct Answer: A, C
Section:
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 23

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

Correct Answer: A, E
Section:

QUESTION 24
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

Correct Answer: B
Section:
Explanation:
http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/shc_qradar_comps.html

QUESTION 25
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

Correct Answer: D
Section:
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 26
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

Correct Answer: B, C
Section:
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 27
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

Correct Answer: A, D
Section:
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 28
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

Correct Answer: C, D
Section:
Explanation:
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 29
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

Correct Answer: B
Section:
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 30
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.

Correct Answer: B, E
Section:
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 31
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

Correct Answer: D
Section:
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 32
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

Correct Answer: C
Section:
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 33
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

Correct Answer: A
Section:
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 34
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.

Correct Answer: A
Section:
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 35
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

Correct Answer: B
Section:
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 36
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

Correct Answer: B, C
Section:
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 37
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

Correct Answer: B
Section:
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 38
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

Correct Answer: C
Section:
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.