PassQueen
a.k.a dumpsqueen.com

IBM Security QRadar SIEM V7.5 Analysis

IBM C1000-162

Version Demo

Total Demo Questions: 15

Total Premium Questions: 155

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, QRadar Overview	28
Topic 2, Offense Analysis	24
Topic 3, Event and Flow Analysis	45
Topic 4, Rules	36
Topic 5, Reports	11
Topic 6, Reference Data	11
Total	155

QUESTION NO: 1

What is the primary use of viewing the Magnitude metric on the Offenses tab?

A. Determine which events to investigate last.

B. Determine the credibility rating that is configured in the log source.

C. Understand the type of offense we are facing.

D. Identify the importance of the offense in your environment.

ANSWER: D

Explanation:

Identify the importance of the offense in your environment. is correct because QRadar uses Magnitude as the overall priority indicator for an offense. Magnitude is calculated from the offense's relevance, severity, and credibility values, producing a normalized score from 0 through 10. This score enables an analyst to quickly understand the relative importance and potential business impact of an offense in the context of the organization, then prioritize triage and investigation accordingly. Relevance incorporates the importance of affected assets and networks, so the same observed activity can receive a different magnitude depending on where it occurs and what it affects. Severity represents the level of threat associated with the event or flow, while credibility reflects QRadar's confidence in the information. Consequently, Magnitude provides a concise, environment-aware way to order offenses and focus response efforts on those that present the most significant risk. IBM describes offense magnitude as a value calculated from these three contributing factors and presents it as a key field for analyzing and prioritizing offenses. See the IBM QRadar documentation on offense magnitude and the IBM guidance for investigating offenses.

QUESTION NO: 2

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 full list of AQL databases, functions and fields (properties) is displayed. In QRadar's Log Activity advanced-search editor, `Ctrl + Space` invokes AQL content assistance. This assistance is intended to help an analyst construct valid Ariel Query Language statements without needing to recall every available item manually. It presents the available AQL databases, supported functions, and searchable fields or properties that can be used in the query context. The capability is especially useful when building expressions for event searches, such as selecting normalized event properties, applying AQL functions, or confirming the names of fields that are available for filtering and aggregation. The displayed list is a query-authoring aid within the advanced search field; it helps the analyst discover and insert recognized AQL elements while composing the search. IBM documents advanced searches as using Ariel Query Language and describes the query-building facilities available from the Log Activity interface. For additional context on AQL query construction and use in QRadar, see the IBM documentation for Ariel Query Language and the IBM documentation for searching events in Log Activity.

QUESTION NO: 3

What are two (2) Y-axis types that are available in the scatter chart type in the Pulse app?

A. Linear

B. Log

C. General

D. Threshold

E. Dynamic

ANSWER: A B

Explanation:

In QRadar Pulse scatter charts, **Linear** and **Log** are the available Y-axis scale types. A linear Y-axis uses equal numerical intervals, so a fixed visual distance represents the same absolute change throughout the chart. This scale is appropriate when values are within a relatively comparable range and analysts need to assess direct differences between plotted values.

A log Y-axis applies logarithmic scaling, meaning equal visual intervals represent multiplicative changes rather than equal absolute changes. It is useful when scatter-plot values span several orders of magnitude, because it makes smaller and larger values more visible in the same chart and helps reveal proportional patterns that might otherwise be obscured. The axis selection therefore controls how Pulse renders the metric values on the vertical dimension; it does not alter the underlying query or data returned to the visualization. IBM's QRadar Pulse documentation describes the chart configuration capabilities available when creating visualizations, including axis settings for supported chart types. See the IBM QRadar Pulse documentation and the QRadar Pulse application listing.

QUESTION NO: 4

Which two (2) dashboards in the Pulse app by default?

A. Active threats

B. System metrics

C. Summary view

D. Compliance overview

E. Offense overview

ANSWER: D E

Explanation:

The Pulse app includes the **Compliance overview** and **Offense overview** dashboards as default dashboard content. The Compliance overview dashboard presents security and regulatory-oriented information in a consolidated visual layout, enabling analysts to monitor compliance-related posture and activity. The Offense overview dashboard provides an at-a-glance operational view of QRadar offenses, helping analysts prioritize and investigate the security incidents that QRadar has correlated from event and flow data. These built-in dashboards demonstrate Pulse's purpose: providing customizable, visual dashboarding for key QRadar security operations and reporting use cases. Administrators and analysts can subsequently customize dashboard layouts, add widgets, and create additional dashboards to suit their organization's monitoring requirements, but these two overview dashboards are supplied as standard Pulse content. IBM's QRadar documentation describes Pulse as the dashboard application for viewing and organizing QRadar data, while the QRadar product documentation explains the central role of offenses in the investigation workflow. See the IBM QRadar Pulse documentation and IBM QRadar offense management documentation.

QUESTION NO: 5 - (SIMULATION)

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: See the explanation for the answer

Explanation:

Use the *Review building blocks* function.

In Use Case Manager, open `Review building blocks` and update the vulnerability-scanner building block (for example, the building block that defines vulnerability scanner source IP addresses). Add the newly deployed scanner IP addresses/ranges to that building block so rules can exclude or appropriately handle scanner activity, reducing the resulting offenses.

QUESTION NO: 6

An analyst wants to share a dashboard in the Pulse app with colleagues.

The analyst exports the dashboard by using which format?

A. CSV

B. JSON

C. XML

D. PHP

ANSWER: B

Explanation:

JSON is the format used when a QRadar Pulse dashboard is exported for sharing. A Pulse dashboard is more than a visual image or a simple table of values: it contains a reusable dashboard definition, including its layout, visualization settings, widget configuration, data queries, and other structured properties. JSON provides a portable, structured representation of that configuration, so another authorized Pulse user can import the exported dashboard definition and work with the same dashboard design in their own QRadar environment. This supports consistent operational views across a security team and avoids rebuilding visualizations manually. The exported JSON file represents the dashboard configuration rather than a one-time report of the currently displayed data. IBM QRadar applications are managed through the QRadar app framework, and Pulse is the dashboarding application used to create and share these configurable visualizations. For IBM documentation about QRadar apps and their administration, see Managing applications in QRadar. Additional QRadar product documentation is available through the IBM QRadar documentation portal.

QUESTION NO: 7

Many offenses are generated and an analyst confirms that they match some kind of vulnerability scanning.

Which building block group needs to be updated to include the source IP of the vulnerability assessment (VA) scanner to reduce the number of offenses that are being generated?

A. Host reference

B. Host definitions

C. Behavior definition

D. Device definition

ANSWER: B

Explanation:

Host definitions is the appropriate building block group because QRadar uses host-definition building blocks to identify known hosts that perform specific, expected functions in the environment. A vulnerability assessment scanner commonly produces large volumes of connection attempts, port probes, and service-discovery activity. Those events can satisfy rule conditions intended to detect reconnaissance or suspicious scanning and can consequently create repeated offenses.

By adding the scanner's source address to the relevant vulnerability-scanner host-definition building block, rules that rely on that known-host context can recognize the activity as originating from an authorized scanner. This permits the applicable QRadar content to handle the scanner's expected behavior appropriately and reduces offense noise, while retaining detection coverage for scanning from hosts that are not identified as approved assessment systems. The entry should use the scanner's actual source address as observed by QRadar, accounting for address translation if applicable, and should be maintained whenever scanner infrastructure changes.

IBM describes building blocks as reusable rule-test components that provide shared context for rules and notes their role in organizing common rule logic. See the IBM QRadar building blocks documentation and the IBM QRadar rule management documentation.

QUESTION NO: 8

Which property types can be used to reduce the overall data volume searched and shorten search time to address searches taking longer than expected?

A. Tabled properties

B. Indexed properties

C. Stored properties

D. Common properties

ANSWER: B

Explanation:

Indexed properties is correct because QRadar can use an index to locate matching events or flows without evaluating every record in the selected time range. When a search filter uses an indexed property, QRadar reduces the amount of data that must be retrieved and processed, which can substantially improve search completion time, especially for high-volume deployments and longer search intervals. Indexing is therefore a key search-optimization technique when the relevant field is known and is frequently used to constrain investigations. In QRadar, administrators can configure custom event properties for indexing where appropriate, then use those properties as search criteria. Effective use requires selecting properties with meaningful values and applying focused filters along with a suitable time range, so that the index can narrow the candidate data set early in search processing. IBM's QRadar administration documentation describes indexed custom properties and their role in supporting faster searches, while IBM's search guidance recommends using indexed fields to optimize search performance. See the IBM documentation on indexing custom event properties and the IBM guidance for optimizing search performance.

QUESTION NO: 9

Which two (2) are valid options available for configuring the frequency of report execution in the QRadar Report wizard?

A. Quarterly

B. Automatically

C. Monthly

D. Yearly

E. Manually

ANSWER: C E

Explanation:

"Monthly" and "Manually" are valid report-execution frequency choices in the QRadar Report wizard. Monthly scheduling is used when a report must be generated on a recurring monthly cycle. This is appropriate for periodic security reporting, such as a monthly summary of offenses, event activity, compliance-related information, or operational metrics. QRadar applies the selected schedule so that the report can be generated without requiring an administrator to initiate each run.

"Manually" is also a supported execution approach. It is intended for reports that should be run on demand rather than according to a recurring schedule. This is useful when an analyst needs an ad hoc report for an investigation, a time-specific review, or a one-time request. Selecting manual execution lets the report definition remain available in QRadar while generation is initiated when it is needed. IBM's QRadar documentation describes report creation and scheduling as part of the Reports workflow; the schedule determines when report output is generated, while manually run reports are initiated by the user. See the IBM QRadar SIEM 7.5 documentation and the IBM documentation on scheduling reports.

QUESTION NO: 10

What type of reference data collection would you use to correlate a unique key to a value?

A. Reference map

B. Reference list

C. Reference table

D. Reference set

ANSWER: A

Explanation:

Reference map is the appropriate QRadar reference-data collection for correlating one unique key with one associated value. A reference map stores entries as key-value pairs, allowing QRadar rules, searches, and reference-data functions to look up a value by its key. For example, a map can associate an IP address or username used as the key with a classification, owner, risk category, or other single value. This structure supports direct enrichment and correlation when the required relationship is a unique identifier mapped to one corresponding item of data.

QRadar reference data is retained independently of event and flow payloads so it can be populated, updated, and queried by correlation content over time. Selecting a reference map ensures that the data model explicitly represents the required one-key-to-one-value relationship, and it enables use of the QRadar reference-map lookup capabilities in custom rules and searches. IBM's QRadar documentation describes reference maps as collections that contain unique keys and their corresponding values, which directly matches the stated requirement. See IBM's Reference data collections documentation and the reference data functions documentation for implementation and lookup details.

QUESTION NO: 11

A security team creates an event rule to identify connections to known malicious IP addresses. When the rule matches, the team needs QRadar to create an investigation and retain the detected source IP address for use by later rules.

Which two (2) rule responses should be configured?

A. Create an offense

B. Add to a reference set

C. Change the QID map

D. Create a custom property

E. Modify the network hierarchy

ANSWER: A B

Explanation:

Create an offense is required to open or contribute to an offense for analyst investigation. **Add to a reference set** stores the selected value, such as the source IP address, in reference data that can be evaluated by subsequent rule tests.

Changing a QID map alters event normalization, not the response to an individual rule match. Creating a custom property is a parsing and extraction task, while modifying the network hierarchy is an administrative network-context configuration task.

QUESTION NO: 12

An analyst is preparing a dashboard for daily triage. The dashboard must show a trend of event volume over time and a ranked view of the log sources generating the most events.

Which two (2) visualization approaches best meet these requirements?

A. A time series chart for event volume

B. A raw payload view for event volume

C. A bar chart grouped by log source

D. An offense note for log source ranking

E. A network hierarchy editor for log source ranking

ANSWER: A C

Explanation:

A time series chart for event volume and **a bar chart grouped by log source** are correct. A time series chart displays how matching records vary across the selected time range, while a bar chart provides a clear comparison of grouped values such as event counts by log source.

A raw payload view is intended for examining individual event content, not summarized dashboard monitoring. An offense note is investigation documentation. A network hierarchy editor is an administrative configuration interface rather than a dashboard visualization.

QUESTION NO: 13

Which action is performed in Edit Search to create a report from Offense data?

A. Under Search Parameters, select "Use Offense Data".

B. In the Select Data Source for report field, select "Offense".

C. In the Data Source field, type offense.

D. Under Search Parameters, select "Associated With Offense Equals True".

ANSWER: B

Explanation:

In QRadar, reports are built by choosing the appropriate report data source before configuring the report content, layout, time range, and delivery settings. Selecting *"Offense"* in the *Select Data Source for report* field establishes that the report query will use offense records rather than event or flow records. Offense records contain the consolidated incident information generated by QRadar correlation, such as offense identifiers, descriptions, categories, assigned users, status, magnitude, source and destination context, and relevant timestamps. This selection is therefore the required action when the intended report is based on offense-level information. After the offense data source is selected, the administrator can apply offense-specific search criteria and choose suitable report elements, such as tables or charts, to present the saved search results. IBM documents report creation as a process that begins with selecting the data source and then defining the report's search and presentation settings. For QRadar SIEM documentation and report-management guidance, see the IBM QRadar SIEM 7.5 documentation and the IBM QRadar reports documentation.

QUESTION NO: 14

What are two (2) axis types available when creating a time series chart?

A. Circular

B. Crossed

C. Linear

D. Log

E. Flat"

ANSWER: C D

Explanation:

Linear and **Log** are the available scale types used for the value axis of a QRadar time series chart. A linear scale uses equal numeric intervals, so an identical vertical distance represents an identical absolute change in the plotted value. This provides a clear representation of ordinary event-count, flow-count, or offense-related trends when values remain within a relatively comparable range. A log scale uses logarithmic intervals, allowing a single chart to represent values that vary by orders of magnitude without the smaller values becoming visually indistinguishable. This is especially useful when a time series includes infrequent high-volume spikes alongside a much lower baseline. Selecting either scale affects the visual interpretation of the measured values over the selected time range; it does not alter the underlying QRadar search results or aggregation. IBM QRadar documentation describes time-series visualization and chart configuration as part of dashboard and app-based data presentation, including the use of appropriate chart settings to make trend data readable. See the IBM QRadar Pulse application documentation and IBM's QRadar documentation search for time series charts.

QUESTION NO: 15

An analyst wants to implement an AQL search in QRadar. Which two (2) tabs can be used to accomplish this implementation?

A. Assets

B. Vulnerabilities

C. Log Activity

D. Offenses

E. Network Activity

ANSWER: C E

Explanation:

QRadar's Ariel Query Language (AQL) is used to query the Ariel data stores that hold event and flow records. The **Log Activity** tab is therefore a primary location for implementing an AQL search against event data. An analyst can use the tab's advanced-search capability to define filters or enter an AQL query that selects event fields, aggregates results, and constrains the time range.

The **Network Activity** tab provides the equivalent AQL-based search capability for network-flow data. Flow searches can use AQL to investigate such information as source and destination addresses, ports, protocols, byte counts, and flow-related custom properties. In both tabs, AQL enables more detailed and repeatable searches than a basic filter-only workflow, and the results can be saved or further investigated in QRadar.

IBM documents AQL as the query language for retrieving and analyzing Ariel event and flow data. The relevant search interfaces are the event-focused Log Activity view and the flow-focused Network Activity view. See IBM's Ariel Query Language documentation and its network flow search documentation.