



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



C1000-162 Dumps
C1000-162 Braindumps
C1000-162 Real Questions
C1000-162 Practice Test
C1000-162 Actual Questions



killexams.com

IBM

C1000-162

IBM Security QRadar SIEM V7.5 Analysis - 2025

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/C1000-162>



Question: 1059

A user is assigned "Edit" permission for firewall log sources but cannot delete log entries. Why?

- A. The user needs "Admin" permission
- B. "Edit" does not include delete rights
- C. The firewall log source is read-only
- D. The user must be in the "Log Managers" group

Answer: B

Explanation: "Edit" permission allows modifications but not deletion of log entries.

Question: 1060

Which process in the QRadar Flow Processor manages the number of incoming flows to comply with licensing restrictions?

- A. License throttling
- B. Asymmetric recombination
- C. Flow deduplication
- D. Forwarding

Answer: A

Explanation: License throttling monitors and manages the number of incoming flows to comply with system licensing.

Question: 1061

In QRadar, you are analyzing a firewall deny event triggered by a rule named "Block_SSH_External." The rule denies SSH traffic (port 22) from external IPs to internal servers. Which AQL query correctly identifies events matching this rule in the last 12 hours, including the rule name and source IP?

- A. SELECT sourceip, rulename FROM events WHERE destinationport = '22' AND rule = 'Block_SSH_External' AND action = 'DENY' LAST 12 HOURS
- B. SELECT sourceip, rule FROM events WHERE destinationport = 22 AND rule = 'Block_SSH_External' AND action = 'DENY' LAST 12 HOURS
- C. SELECT sourceip, rulename FROM events WHERE port = '22' AND rulename = 'Block_SSH_External' AND deny = 'true' LAST 12 HOURS
- D. SELECT sourceip, rulename FROM events WHERE destinationport = '22' AND rulename = 'Block_SSH_External' AND action = 'DENY' LAST 12 HOURS

Answer: D

Explanation: The correct AQL query uses SELECT sourceip, rulename to retrieve specific fields, WHERE destinationport = '22' to filter for SSH traffic, rulename = 'Block_SSH_External' to match the rule name, and action = 'DENY' to confirm the deny action. The LAST 12 HOURS clause sets the time range. The option SELECT sourceip, rule FROM events uses an incorrect field name (rule instead of rulename). The option SELECT sourceip, rulename FROM events WHERE port = '22' uses an invalid field (port instead of destinationport). The option SELECT sourceip, rulename FROM events WHERE destinationport = '22' AND rule = 'Block_SSH_External' also uses the incorrect field name rule.

Question: 1062

A QRadar deployment is experiencing performance issues due to high event rates. An analyst needs to optimize a rule that triggers on port scan activity from a single source IP to multiple destination ports. Which two modifications can improve rule performance?

- A. Enable rule response limiter to cap triggers per hour
- B. Index the DESTINATIONPORT field in the offense index
- C. Reduce the rule's time window from 5 minutes to 1 minute
- D. Use a reference set to store known scanner IPs

Answer: A, B

Explanation: Enabling a rule response limiter caps the number of triggers per hour, reducing system load. Indexing the DESTINATIONPORT field in the offense index speeds up queries for port scan detection, as it optimizes searches on this field. Reducing the time window may increase false negatives by missing slower scans. Using a reference set for scanner IPs is useful for filtering but does not directly improve rule performance.

Question: 1063

Which two (2) commands are required to move data from the old to the new storage location during migration?

- A. `mv -f /store_old/* /store`
- B. `cp -af /store_old/* /store`
- C. `rm -rf /store_old`
- D. `mount /store`
- E. `umount /store_old`

Answer: A, D

Explanation: The `mv -f /store_old/* /store` command moves data, and `mount /store` attaches the new storage; `cp -af` copies data (not move), `rm -rf` deletes, and `umount` detaches the old mount.

Question: 1064

A security rule must test if a network connection is approved in the organization. Which building blocks should the rule reference?

- A. BB:HostDefinition and BB:HostReference
- B. BB:PortAssignment and BB:ProtocolType
- C. BB:ReferenceSet and BB:PortList
- D. BB:AssetProfile and BB:NetworkHierarchy

Answer: A

Explanation: BB:HostDefinition and BB:HostReference building blocks are used to signal approved network connections in QRadar.

Question: 1065

An organization wants to detect DDoS attacks by aggregating many-to-one flows into a single superflow. Which threshold parameter should be configured on the Flow Collector?

- A. Type A Superflows
- B. Type B Superflows

- C. Type C Superflows
- D. Maximum Data Capture/Package

Answer: B

Explanation: Type B Superflows are used to aggregate many-to-one flows, which is typical in DDoS attack scenarios.

Question: 1066

A SOC analyst is investigating a series of failed queries with the error: "AQL query timeout." The query is:

```
SELECT SOURCEIP, DESTINATIONIP, QIDNAME(qid) as EventName FROM events  
WHERE PAYLOAD ILIKE '%timeout%' LAST 7 DAYS
```

Which two changes could prevent the timeout error?

- A. Reduce the time range to LAST 1 DAY.
- B. Add an index on the PAYLOAD column.
- C. Use UTF8(payload) instead of PAYLOAD in the WHERE clause.
- D. Filter by specific QIDNAME values before applying the ILIKE condition.

Answer: A, D

Explanation: Reducing the time range to LAST 1 DAY decreases the dataset size, reducing processing time and preventing timeouts. Filtering by specific QIDNAME values narrows the query scope, improving performance. The PAYLOAD column cannot be indexed in QRadar, and while UTF8(payload) is correct for payload searches, it doesn't directly address the timeout issue.

Question: 1067

Which action is necessary to manually add a host to a building block if it is not automatically detected during server discovery?

- A. Add the host to the port configuration file
- B. Edit the reference set and insert the host name
- C. Double-click the appropriate Host Definition Building Block and add the IP or CIDR
- D. Update the network hierarchy in the Admin tab

Answer: C

Explanation: To manually add a host, double-click the appropriate Host Definition Building Block and enter the host's IP address or CIDR.

Question: 1068

Which configuration enables auto-refresh for a dashboard chart every 5 minutes?

- A. Set Auto-Refresh Interval: 5 minutes in Chart Settings
- B. Enable Auto-Refresh, set Interval: 5 minutes in Dashboard Settings
- C. On the dashboard item, click Settings, set Auto-Refresh Interval: 5 minutes
- D. Click Settings, enable Auto-Refresh, set Refresh Rate: 5 minutes

Answer: C

Explanation: Auto-refresh is configured at the dashboard item level by setting the interval in the item's settings.

Question: 1069

An analyst needs to create an AQL query to identify flows where the source IP is in a reference set "Suspicious_IPs" and the total bytes exceed 10MB in the last 6 hours. Which query is correct?

- A. `SELECT sourceip, SUM(bytes) as total_bytes FROM flows WHERE sourceip IN REFERENCESET 'Suspicious_IPs' GROUP BY sourceip HAVING total_bytes > 10000000 LAST 6 HOURS`
- B. `SELECT sourceip, SUM(bytes) FROM flows WHERE sourceip IN 'Suspicious_IPs' GROUP BY sourceip HAVING SUM(bytes) > 10000000 LAST 6 HOURS`
- C. `SELECT sourceip, SUM(bytes) as total_bytes FROM flows WHERE sourceip MATCHES 'Suspicious_IPs' GROUP BY sourceip HAVING total_bytes > 10000000 LAST 6 HOURS`
- D. `SELECT sourceip, COUNT(bytes) as total_bytes FROM flows WHERE sourceip IN REFERENCESET 'Suspicious_IPs' GROUP BY sourceip HAVING total_bytes > 10000000 LAST 6 HOURS`

Answer: A

Explanation: To identify flows with source IPs in the "Suspicious_IPs" reference set and total bytes exceeding 10MB (10,000,000 bytes), the query must use IN REFERENCESET and SUM(bytes) with HAVING. The option SELECT sourceip, SUM(bytes) as total_bytes FROM flows WHERE sourceip IN REFERENCESET 'Suspicious_IPs' GROUP BY sourceip HAVING total_bytes > 10000000 LAST 6 HOURS is correct. The option SELECT sourceip, SUM(bytes) FROM flows WHERE sourceip IN 'Suspicious_IPs' is incorrect because IN without REFERENCESET is invalid. The option SELECT sourceip, SUM(bytes) as total_bytes FROM flows WHERE sourceip MATCHES 'Suspicious_IPs' is incorrect because MATCHES is not valid. The option SELECT sourceip, COUNT(bytes) as total_bytes FROM flows is incorrect because COUNT(bytes) does not sum bytes.

Question: 1070

Which two (2) steps are required before mounting a new storage partition for QRadar data?

- A. Create the mount point directory
- B. Add the UUID to /etc/fstab
- C. Export offenses as CSV
- D. Run update-ca-trust
- E. Restart the crond service

Answer: A, B

Explanation: Creating the mount point directory and adding the UUID to /etc/fstab are required before mounting a new storage partition; exporting offenses, running update-ca-trust, and restarting crond are not required.

Question: 1071

A QRadar system is configured to auto-refresh log activity every 1 minute. The analyst notices that log data from a specific log source is missing. Which command can be used to verify the log source's connectivity?

- A. /opt/qradar/support/test_logsource.sh
- B. /opt/qradar/bin/check_logsource.sh
- C. /opt/qradar/support/logsource_connectivity.sh

D. /opt/qradar/bin/verify_source.pl

Answer: A

Explanation: The /opt/qradar/support/test_logsource.sh command tests connectivity to a specific log source, helping diagnose missing log data issues. The other commands (logsource_connectivity.sh, check_logsource.sh, verify_source.pl) do not exist in QRadar.

Question: 1072

An analyst needs to create a QRadar rule to detect traffic from a host definition building block (BB:DatabaseServers) to ports in a reference set (RestrictedPorts). Which AQL query should be used to test this rule?

- A. SELECT * FROM events WHERE sourceIP IN BB:HostDefinition:DatabaseServers AND destinationPort IN REFERENCESET('RestrictedPorts')
- B. SELECT sourceIP, destinationPort FROM flows WHERE sourceIP IN BB:DatabaseServers AND destinationPort IN RestrictedPorts
- C. SELECT * FROM events WHERE sourceIP = BB:DatabaseServers AND destinationPort IN REFERENCESET('RestrictedPorts')
- D. SELECT sourceIP FROM events WHERE sourceIP IN BB:HostDefinition:DatabaseServers AND destinationPort = REFERENCESET('RestrictedPorts')

Answer: A

Explanation: The AQL query SELECT * FROM events WHERE sourceIP IN BB:HostDefinition:DatabaseServers AND destinationPort IN REFERENCESET('RestrictedPorts') correctly retrieves events from hosts in the DatabaseServers building block communicating on ports in the RestrictedPorts reference set. Using flows instead of events is incorrect, sourceIP = BB:DatabaseServers is invalid syntax, and destinationPort = REFERENCESET('RestrictedPorts') is incorrect, as = is not used for reference set comparisons.

Question: 1073

An analyst is tasked with creating an AQL query to find events where the destination port is 443 and the event payload contains both "login" and "failed" keywords. Which two

queries would correctly retrieve this data?

- A. SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login%failed%'
- B. SELECT * FROM events WHERE destinationport = 443 AND payload CONTAINS 'login' AND payload CONTAINS 'failed'
- C. SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login%' AND payload ILIKE '%failed%'
- D. SELECT * FROM events WHERE destinationport = 443 AND payload LIKE '%login%failed%'
- E. SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login% AND %failed%'

Answer: C

Explanation: To find events with destination port 443 and payloads containing both "login" and "failed," the query must use ILIKE for case-insensitive matching and separate conditions for each keyword. The option SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login%' AND payload ILIKE '%failed%' is correct, as it checks for both keywords independently. The option SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login%failed%' is incorrect because it searches for the exact string "loginfailed," not separate keywords. The option SELECT * FROM events WHERE destinationport = 443 AND payload CONTAINS 'login' AND payload CONTAINS 'failed' is incorrect because CONTAINS is not a valid AQL keyword. The option SELECT * FROM events WHERE destinationport = 443 AND payload LIKE '%login%failed%' is incorrect because LIKE is case-sensitive. The option SELECT * FROM events WHERE destinationport = 443 AND payload ILIKE '%login% AND %failed%' uses invalid syntax for multiple ILIKE conditions.

Question: 1074

An analyst needs to tune a QRadar rule that triggers offenses with high event counts (500+) but low magnitude (4). Which adjustment would most effectively increase the offense magnitude for relevant threats?

- A. Increase the rule's severity value
- B. Decrease the event threshold in the rule
- C. Modify the log source's parsing settings
- D. Update the network hierarchy's asset weights

Answer: A

Explanation: To increase the offense magnitude for relevant threats, the analyst should increase the rule's severity value. Since magnitude is calculated as $(\text{Severity} \times \text{Asset Weight}) + \text{Credibility}$, a higher severity directly increases the magnitude. Decreasing the event threshold may increase event counts but not magnitude, modifying parsing settings affects credibility, and updating asset weights is less targeted than adjusting severity.

Question: 1075

An analyst is troubleshooting a query that fails to execute:

```
SELECT SOURCEIP, QIDNAME(qid) as EventName FROM events WHERE  
QIDNAME(qid) = 'System Error' AND PAYLOAD CONTAINS 'critical' LAST 1 DAY
```

The error message is: "Invalid operator: CONTAINS." How should the query be corrected?

- A. Change QIDNAME(qid) to EVENTNAME(qid).
- B. Use PAYLOADTEXT instead of PAYLOAD.
- C. Add a semicolon at the end of the query.
- D. Replace CONTAINS with ILIKE '%critical%'.

Answer: D

Explanation: AQL does not support the CONTAINS operator; the correct operator for string matching is ILIKE with wildcards (e.g., ILIKE '%critical%'). PAYLOADTEXT is valid but not required here, a semicolon is not needed, and EVENTNAME(qid) is not a valid function.

Question: 1076

A security analyst needs to configure a log source in QRadar to auto-refresh log data every 2 minutes while ensuring log files are parsed correctly for a custom application. Which two configuration settings must be adjusted in the Log Source Management app to achieve this?

- A. Coalescing Events
- B. Log File Retention Period
- C. Polling Interval
- D. Protocol Configuration

E. Storage Location

Answer: C, D

Explanation: To configure a log source for auto-refreshing log data every 2 minutes, the analyst must set the Polling Interval to 120 seconds in the Log Source Management app to control how frequently QRadar polls the log source for new data. Additionally, the Protocol Configuration must be adjusted to ensure the correct protocol (e.g., Syslog, FTP) is used to retrieve and parse the log files correctly for the custom application. Coalescing Events affects event grouping, not refresh timing. Log File Retention Period determines how long logs are stored, not refresh frequency. Storage Location specifies where logs are stored, which is unrelated to polling or parsing.

Question: 1077

Which two (2) statements about offense chaining are true? (Select two.)

- A. Offense chaining allows linking related offenses via index fields
- B. Offense chaining is enabled by default for all rule types
- C. Offense chaining uses the offense index field to group offenses
- D. Offense chaining requires manual intervention to link offenses

Answer: A, C

Explanation: Offense chaining links related offenses using the offense index field, and this process is automatic for rules configured with chaining.

Question: 1078

An analyst is tasked with creating a reference set to store file hashes of known malware. Entries must be retained for 365 days, but those inactive for 90 days should be purged unless they are referenced in an offense with a specific severity level. The analyst also needs to ensure the reference set is populated from a CSV file uploaded periodically. Which steps should the analyst follow?

- A. Create reference set, set Time to Live to 365 days, enable Conditional Purge, set Inactivity Timeout to 90 days, configure CSV upload in Reference Set Management
- B. Create reference set, set Expiration to 365 days, enable Purge on Inactivity, set Reference Timeout to 90 days, configure CSV upload in Log Activity
- C. Create reference set, set Time to Live to 90 days, enable Purge on Reference, set Expiration to 365 days, configure CSV upload in Use Case Manager
- D. Create reference set, set Expiration to 90 days, disable Conditional Purge, set

Reference Check to 365 days, configure CSV upload in Pulse

Answer: A

Explanation: The Time to Live setting of 365 days ensures file hashes are retained for 365 days. Enabling Conditional Purge with an Inactivity Timeout of 90 days allows purging of inactive entries unless they are referenced in an offense with a specific severity level. In QRadar, CSV uploads for reference sets are configured in the Reference Set Management interface. The other options misuse Expiration or configure CSV uploads in incorrect interfaces.

Question: 1079

An analyst is tasked with creating a dashboard item to show the top 5 source IPs with the highest flow rates, using a column chart with a logarithmic Y-axis and a 10-minute refresh interval. Which configuration is correct?

- A. Add a Column Chart, set Y-Axis to Logarithmic, use AQL query `SELECT SOURCEIP, SUM(BYTES) FROM flows GROUP BY SOURCEIP ORDER BY SUM(BYTES) DESC LIMIT 5`, set refresh to 600 seconds
- B. Configure a Line Chart, use a linear Y-axis, and apply a global filter for source IPs
- C. Use Pulse app to import a flow template and modify the Y-axis
- D. Create a saved search in Network Activity and pin it to the dashboard

Answer: A

Explanation: For a dashboard item showing the top 5 source IPs by flow rates, a Column Chart is appropriate. The AQL query `SELECT SOURCEIP, SUM(BYTES) FROM flows GROUP BY SOURCEIP ORDER BY SUM(BYTES) DESC LIMIT 5` calculates total bytes per source IP. Setting the Y-Axis to Logarithmic accommodates varying flow rates, and a 600-second (10-minute) refresh interval ensures periodic updates. A Line Chart with a linear Y-axis is unsuitable for ranking data. The Pulse app is not the primary method for custom dashboards. Pinning a saved search lacks the specific chart configuration required.

Question: 1080

A log source is configured with a Log Source Extension. When is this parameter visible?

- A. Only for IPv6 log sources
- B. Always, regardless of configuration
- C. Only if a log source extension is configured in the deployment
- D. When the log source is disabled

Answer: C

Explanation: The Log Source Extension parameter is visible only if a log source extension is configured in the deployment.

Question: 1081

An analyst needs to export offenses to a CSV file and split the output by offense severity (Low, Medium, High). Which command achieves this?

- A. `/opt/qradar/support/export_offense --format CSV --by_severity`
- B. `/opt/qradar/bin/offense_export.py --type CSV --group severity`
- C. `/opt/qradar/bin/export_offenses.sh --format csv --split_by severity`
- D. `/opt/qradar/bin/export_offenses.sh --format csv --group_by severity`

Answer: C

Explanation: The command `/opt/qradar/bin/export_offenses.sh --format csv --split_by severity` splits the CSV output by offense severity. The other commands are either invalid or use incorrect parameters.



KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:



Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.