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

KILL EXAMS

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

PASS

killexams.com

IBM

C1000-162

IBM Certified Analyst - Security QRadar SIEM V7.5 (Code: C9005200)

ORDER FULL VERSION

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

Question: 1

When designing rules in QRadar, which option allows for matching an event to a specific set of criteria?

A. Regex patterns
B. Reference sets
C. Custom properties
D. Log sources

Answer: A

Explanation: Regex patterns in QRadar enable the matching of events to a specific set of criteria. Regular expressions provide a powerful and flexible way to define patterns for identifying and correlating events based on specific conditions or characteristics.

Question: 2

Which tab in IBM Security QRadar SIEM allows an analyst to manage the layout and content of dashboards?

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

Answer: D

Explanation: The Dashboard tab in IBM Security QRadar SIEM allows an analyst to manage the layout and content of dashboards. Analysts can add, remove, and arrange widgets, as well as customize the visualizations and data sources used in the dashboards.

Question: 3

What is the purpose of correlation rules in IBM Security QRadar SIEM?

A. To define the severity levels of offenses.
B. To link related events and generate offenses.
C. To classify events into different categories.
D. To filter out false positive events.

Answer: B

Explanation: Correlation rules in IBM Security QRadar SIEM are used to link related events and generate offenses. They define the conditions and patterns that, when met, indicate a potential security incident or threat.

Question: 4

What is the purpose of the "LIKE" operator in event searching within IBM Security QRadar SIEM?

A. To search for events that are similar to a given event.
B. To search for events that contain a specific keyword or pattern.
C. To search for events that are associated with a specific offense.
D. To search for events that occurred within a specific time range.

Answer: B

Explanation: The "LIKE" operator in event searching within IBM Security QRadar SIEM is used to search for events that contain a specific keyword or pattern. It allows analysts to identify events of interest based on specific terms or patterns within the event data.

Question: 5

How can an analyst export a search result as a report in IBM Security QRadar SIEM?

A. Use the "Export" button in the search results page.
B. Write a custom script to extract the search result data.
C. Use the QRadar API to generate a report programmatically.
D. Copy and paste the search result into a separate document.

Answer: A

Explanation: Analysts can export a search result as a report in IBM Security QRadar SIEM by using the"Export" button in the search results page. This allows the analyst to save the search result data in a format suitable for reporting and further analysis.

Question: 6

What is the purpose of building blocks in IBM Security QRadar SIEM?

A. To define custom parsing rules for log sources.
B. To create custom correlation rules for offenses.
C. To design custom dashboards for reporting.
D. To configure threat intelligence feeds for threat hunting.

Answer: B

Explanation: Building blocks in IBM Security QRadar SIEM are used to create custom correlation rules for offenses. These rules define specific conditions and events that, when met, trigger the generation of an offense.

Question: 7

Which tab in IBM Security QRadar SIEM allows an analyst to search for events based on specific criteria?

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

Answer: B

Explanation: The Log Activity tab in IBM Security QRadar SIEM allows an analyst to search for events based on specific criteria. Analysts can apply filters, keywords, time ranges, and other parameters to narrow down the search results.

Question: 8

How can an analyst create a custom dashboard in IBM Security QRadar SIEM?

A. Use the built-in dashboard templates and modify them as needed.
B. Write custom SQL queries to fetch data for the dashboard.
C. Use the QRadar API to develop a custom web-based dashboard.
D. Import pre-built dashboards from the IBM Security App Exchange.

Answer: A

Explanation: Analysts can create a custom dashboard in IBM Security QRadar SIEM by using the built-in dashboard templates and modifying them as needed. The system provides a range of widgets and visualization options that can be tailored to display relevant information.

Question: 9

Which component of IBM Security QRadar SIEM is responsible for analyzing offenses and generating alerts?

A. Event Processor
B. Flow Processor
C. Offense Analyzer
D. Event Collector

Answer: C

Explanation: The Offense Analyzer is the component in IBM Security QRadar SIEM that is responsible for analyzing offenses and generating alerts based on the rules and building blocks configured in the system.

Question: 10

Which component of IBM Security QRadar SIEM is responsible for generating offenses?

A. Event Collector
B. Event Processor
C. Flow Processor
D. Offense Analyzer

Answer: B

Explanation: The Event Processor component in IBM Security QRadar SIEM is responsible for processing incoming events, normalizing them, and generating offenses based on the configured rules and building blocks.

SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

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.*