QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

000-N24 Dumps
000-N24 Braindumps
000-N24 Real Questions
000-N24 Practice Test
000-N24 dumps free

IBM

# 000-N24

*IBM QRadar Technical Sales Mastery Test v1*

**QUESTION:** 35
What does the ecs process do?

A. Control event collection
B. Control the GUI
C. Contains host vulnerabilities
D. Process flow data

**Answer:** A:

**QUESTION:** 36
How do you filter the information that is seen in the Log Activity window?

A. Right click the column and select filter.
B. Use the dd Filter?button on the toolbar.Use the ?dd Filter?button on the toolbar.
C. Write xml wrappers and apply them to the events window.
D. Use dit search.?Use ?dit search.
E. A, B, and D are correct.

**Answer:** E:

**QUESTION:** 37
What is a custom property?

A. A method of defining a regular expression to extract specific data from an event payload. It can be used to display the data in reports and searches and in rules.
B. A method of telling QRadar to parse information in a different way and use a different field in the Ariel database to store it.
C. A method of renaming a field in an event payload modifying the original data.
D. A method of using regular expressions to add custom users.

**Answer:** A:

**QUESTION:** 38
What problems might Log Source Extensions cause?

A. Break the flow collector
B. Increase the QFlow packet capture size
C. Impact on the system performance
D. Make the system look untidy

**Answer:** C:

**QUESTION:** 39
What is a DSM?

A. A Device Signature Manager which matches security alerts to categories.
B. A Data Solutions Module that allows you to add extra fields to an event.
C. A Device Support Module which maps events and data within them to specific fields.
D. A Daemon System Manager that can be used to control the processes running on QRadar.

**Answer:** C:

**QUESTION:** 40
How might you use a Building Block?

A. As a part of a complex rule.
B. In a multi part rule to simplify the rule.
C. As a pivot for assessing offense and sentry data.
D. Both A and B are correct.

**Answer:** D:

**QUESTION:** 41
What is the difference between ave Criteria?and ave Results?What is the difference between ?ave Criteria?and ?ave Results?

A. There is no difference between ave Criteria?and ave Results.?There is no difference between ?ave Criteria?and ?ave Results.

B. ave Criteria?saves the filters on a search and makes the search available for future use. ?ave Criteria?saves the filters on a search and makes the search available for future use. ave Results?saves the results of a search and makes them available for future use.?ave Results?saves the results of a search and makes them available for future use.
C. ave Criteria?saves the results of a search in xml or csv format.?ave Criteria?saves the results of a search in xml or csv format. ave Results?stores the raw log data as a template.?ave Results?stores the raw log data as a template.
D. ave Criteria?saves future searches in the system. ?ave Criteria?saves future searches in the system. ave Results?only works when indexing is enabled.?ave Results?only works when indexing is enabled.

**Answer:** B:

**QUESTION:** 42
In what formats can you export viewer data?

A. pdf and html
B. xml and html
C. txt and Microsoft word
D. csv and xml

**Answer:** D