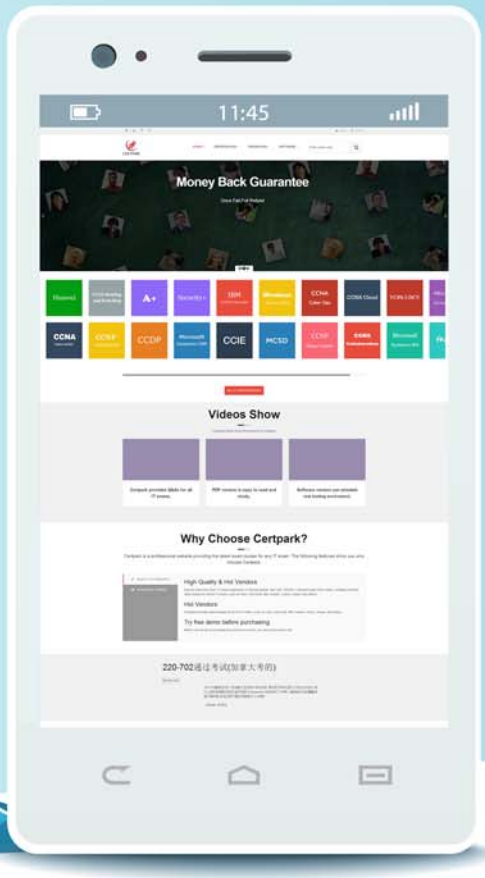
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **C1000-018**

Title : IBM QRadar SIEM V7.3.2 Fundamental Analysis

Version : DEMO

1.How many normalized timestamp field(s) does an event contain?
A. 2
B. 3
C. 4
D. 1
Answer: B
Explanation:
There are 3 timestamp fields on events in Qradar.
Reference:
https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-different-time-stamps-for-qradar-events?language=en_US

2.What information is included in flow details but is not in event details?
A. Network summary information
B. Magnitude information
C. Number of bytes and packets transferred
D. Log source information
Answer: A
Explanation:
Flows represent network activity by normalizing IP addresses, ports, byte and packet counts, and other data, into flow records, which effectively are records of network sessions between two hosts.
Reference: https://www.ibm.com/docs/en/qsip/7.3.2?topic=overview-qradar-events-flows

3.An analyst is working on Offense management and finds that a few of the offenses are not being removed from the Offense tab even after the Offense retention period has elapsed.
What could be the reason that these offenses are not being removed?
A. Offense has been annotated
B. Offense is inactive
C. Offense is released
D. Offense is protected
Answer: D
Explanation:
https://www.ibm.com/docs/en/qsip/7.4?topic=management-offense-retention

4.An analyst is searching for a list of events that meet specific search criteria and wants to display only the source IP and destination IP information for the events.
To get the required information, the analyst can open the Log Activity tab and then:
A. select the field names, select the start and end time from the drop down fields in the filters section, then click search.
B. click add filter, select the desired parameters, operators, values and field names, then click search.
C. select advanced search, type the corresponding AQL query, then click search.
D. select search, then new search, scroll down and select time range, column definitions, the search parameters then click search.
Answer: A

5.When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?

A. When the source is [local or remote]

B. When the destination is [local or remote]

C. When the event(s) were detected by one or more of [these log sources]

D. When an event matches all of the following [Rules or Building Blocks]

Answer: A