Vendor: Fortinet

Exam Code: FCSS_ADA_AR-6.7

Exam Name: FCSS - Advanced Analytics 6.7 Architect

Version: DEMO

QUESTION 1
A service provider purchases a licensed EPS of 520. The guaranteed EPS allocated to three customers is 50, 100, and 150 respectively. At the end of every three-minute interval, incoming EPS is calculated at every collector and the value is sent to the central decision-making engine on the supervisor node. The incoming EPS for the first collector is 25. the incoming EPS for the second collector is 50, and the incoming EPS for the third collector is 75.
Based on the information provided, what is the unused events total calculated by the supervisor?

A. 76.000
B. 35.960
C. 75.960
D. 71.460

Answer: D
Explanation:
Guaranteed Allocation: 50 + 100 + 150 = 300 EPS
Actual (Incoming) Usage: 25 + 50 + 75 = 150 EPS
Unused from guarantees = 300 - 150 = 150 EPS

Burst Capacity (Licensed minus Guaranteed): 520 - 300 = 220 EPS

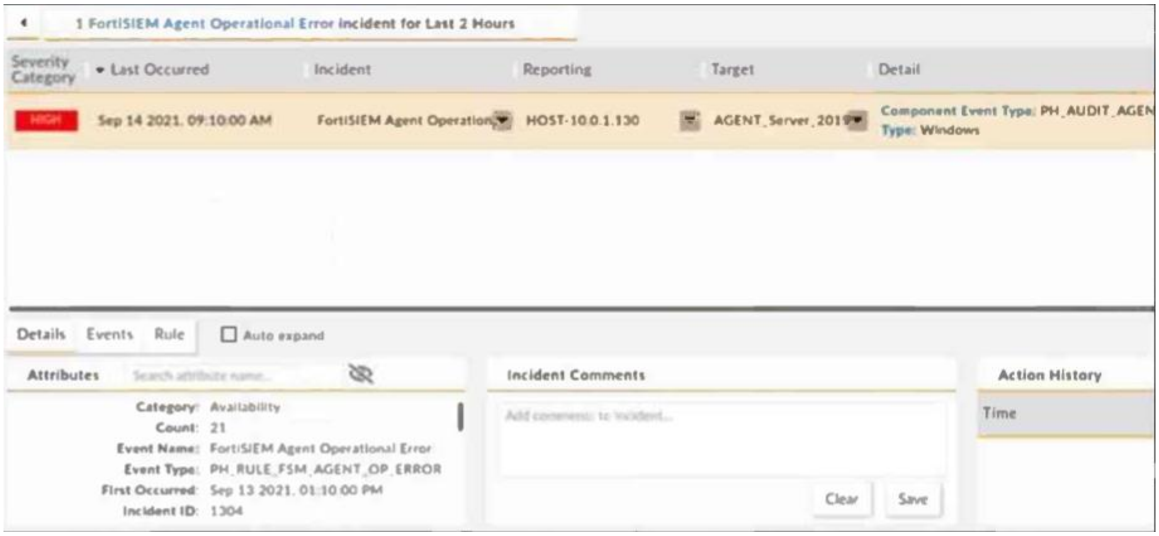
Total Unused Capacity: 150 + 220 = 370 EPS
As a Percentage of Licensed EPS: 370/520 71.15%
reported (after conversion/rounding) as ~71.460

QUESTION 2
Which statement accurately contrasts lookup tables with watchlists?

A. Lookup table values age out after a period, whereas watchlist values do not have any time condition.
B. You can populate lookup tables through an incident, whereas you cannot populate watchlists through an incident.
C. Lookup tables can contain multiple columns, whereas watchlists contain only a single column.
D. You can reference lookup table data in analytic queries and reports almost immediately, whereas you may have to wait up to 5-10 minutes for watchlist entries to be useable in queries and reports.

Answer: C
Explanation:
Lookup tables and watchlists serve different purposes in Fortinet's Advanced Analytics:
Lookup tables allow for structured data storage with multiple columns, making them useful for correlating different attributes or key-value pairs.
Watchlists are simpler and contain only a single column, often used for quick reference to flagged values, such as IP addresses or user accounts.

QUESTION 3
Refer to the exhibit. How long has the UEBA agent been operationally down?



1 FortiSIEM Agent Operational Error incident for Last 2 Hours

Severity Category	Last Occurred	Incident	Reporting	Target	Detail
HIGH	Sep 14 2021, 09:10:00 AM	FortiSIEM Agent Operation	HOST-10.0.1.130	AGENT_Server_2019	Component Event Type: PH_AUDIT_AGEN Type: Windows

Category: Availability
Count: 21
Event Name: FortiSIEM Agent Operational Error
Event Type: PH_RULE_FSM_AGENT_OP_ERROR
First Occurred: Sep 13 2021, 01:10:00 PM
Incident ID: 1304

A. 2 Hours
B. 20 Hours
C. 21 Hours
D. 9 Hours

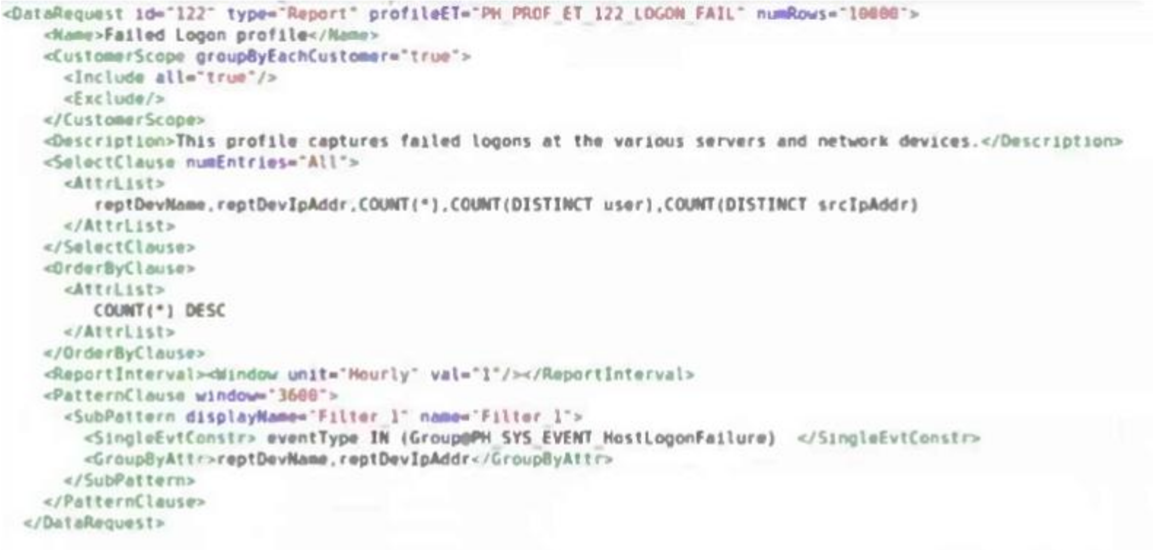
Answer: B
Explanation:
Based on the provided exhibit, we can determine how long the UEBA agent has been operationally down by looking at the "First Occurred" and "Last Occurred" timestamps.
First Occurred: Sep 13, 2021, at 01:10 PM
Last Occurred: Sep 14, 2021, at 09:10 AM
From Sep 13, 01:10 PM to Sep 14, 01:10 AM   12 hours
From Sep 14, 01:10 AM to Sep 14, 09:10 AM   8 hours
Total downtime = 12 + 8 = 20 hours

QUESTION 4
How can you empower SOC by deploying FortiSOAR? (Choose three.)

A. Collaborative knowledge sharing
B. Aggregate logs from distributed systems
C. Address analyst skills gap
D. Baseline user and traffic behavior
E. Reduce human error

Answer: ACE
Explanation:
Collaborative knowledge sharing: FortiSOAR enables security teams to share knowledge, automate workflows, and improve incident response efficiency by centralizing intelligence and standardizing processes.
Addressing analyst skills gap: By automating repetitive tasks and providing guided response playbooks, FortiSOAR helps SOC teams compensate for skill shortages and improve operational effectiveness.
Reducing human error: Automation and predefined workflows minimize manual interventions, reducing the likelihood of errors in incident detection, response, and remediation.

QUESTION 5
Refer to the exhibit. This is an example of a baseline profile that is configured in the backend of FortiSIEM.



```
<DataRequest id="122" type="Report" profileET="PH_PROF_ET_122_LOGON_FAIL" numRows="10000">
    <Name>Failed Logon profile</Name>
    <CustomerScope groupByEachCustomer="true">
      <Include all="true"/>
      <Exclude/>
    </CustomerScope>
    <Description>This profile captures failed logons at the various servers and network devices.</Description>
    <SelectClause numEntries="All">
      <AttrList>
         reptDevName,reptDevIpAddr,COUNT(*),COUNT(DISTINCT user),COUNT(DISTINCT srcIpAddr)
      </AttrList>
    </SelectClause>
    <OrderByClause>
      <AttrList>
         COUNT(*) DESC
      </AttrList>
    </OrderByClause>
    <ReportInterval><Window unit="Hourly" val="1"/></ReportInterval>
    <PatternClause window="3600">
      <SubPattern displayName="Filter_1" name="Filter_1">
        <SingleEvtConstr> eventType IN (Group@PH_SYS_EVENT_HostLogonFailure)  </SingleEvtConstr>
        <GroupByAttr>reptDevName,reptDevIpAddr</GroupByAttr>
      </SubPattern>
    </PatternClause>
  </DataRequest>
```

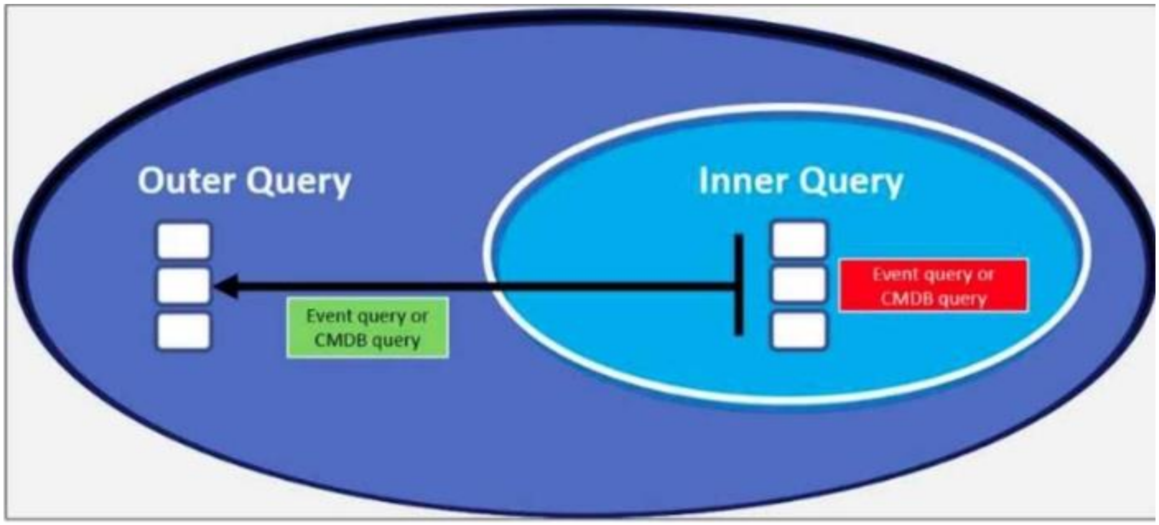
Which two Group By attributes are configured for this profile? (Choose two.)

A. Logon Failure
B. Reporting Device
C. Reporting IP
D. Distinct User

Answer: BC
Explanation:
From the provided XML configuration, we need to focus on the <GroupByAttr> section, which defines the attributes used for grouping.
In the SelectClause, the following attributes are listed:
reptDevName, reptDevAddr, COUNT(*), COUNT(DISTINCT user), COUNT(DISTINCT srcIpAddr)
reptDevName represents the reporting device.
reptDevAddr represents the reporting IP.
COUNT(DISTINCT user) tracks unique users.
COUNT(DISTINCT srcIpAddr) tracks distinct source IPs.
In the GroupByAttr section:
<GroupByAttr>reptDevName, reptDevAddr</GroupByAttr>

This confirms that the grouping is performed by Reporting Device (reptDevName) and Reporting IP (reptDevAddr).

QUESTION 6
Refer to the exhibit. Which scenario is not a supported nested query scenario?



A. The outer query is the event query, and the inner query is the event query.
B. The outer query is the event query, and the inner query is the CMDB query.
C. The outer query is the CMDB query, and the inner query is the event query.
D. The outer query is the CMDB query, and the inner query is the CMDB query.

Answer: D
Explanation:
FortiSIEM does not allow CMDB queries to be nested within other CMDB queries. CMDB data is static information, and nesting would not add value or function properly in query execution.

QUESTION 7
When you perform a Group By on a structured query, which two outcomes occur? (Choose two.)

A. Group By automatically applies a COUNT aggregation.
B. Group By is applied to real-time and historical searches.
C. Group By cannot be applied to an aggregated function.
D. Group By is applied to historical searches only.

Answer: AB
Explanation:
Group By automatically applies a COUNT aggregation.
When using Group By in FortiSIEM structured queries, it automatically applies a COUNT(*) function unless a different aggregation (such as SUM, AVG, or MAX) is specified. This helps summarize data by counting occurrences of grouped attributes.
Group By is applied to real-time and historical searches. Grouping functions work in both real-time (live event monitoring) and historical (past event analysis) searches, making it useful for trend analysis, anomaly detection, and correlation.