DUMPSARENA

FCSSAdvanced Analytics 6.7 Architect

Fortinet FCSS_ADA_AR-6.7

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSIEM	23
Total	23

QUESTION NO: 1

Which three processes are collector processes? (Choose three.)

A. phParser

B. phAgentManager

C. phMonitorAgent

D. phReportMaster

E. phRuleMaster

ANSWER: A B C

Explanation:

phParser, **phAgentManager**, and **phMonitorAgent** are collector processes in FortiSIEM. A Collector is responsible for receiving event data from monitored devices and agents, processing that data locally as needed, and forwarding it to the Supervisor for storage, correlation, and analytics. **phParser** performs the event parsing function, converting received raw events into FortiSIEM's normalized event representation so that the events can be used consistently for search, reporting, and analytics. **phAgentManager** supports communication with FortiSIEM agents, including receiving agent-provided event and status information. **phMonitorAgent** provides node and service health-monitoring information, enabling the FortiSIEM deployment to monitor the operational status of the Collector. Together, these services support the Collector's acquisition, parsing, agent-management, and health-monitoring responsibilities. Fortinet's product documentation describes FortiSIEM deployment roles and operational architecture in the FortiSIEM 6.7 documentation; Fortinet's FortiSIEM 6.7 Administration Guide provides further administration and service-operation context.

QUESTION NO: 2

A baseline profile must identify an unusual number of failed logons for each user on each reporting device. The same user can legitimately have very different authentication patterns on different systems.

Which two attributes should be configured as Group By attributes? (Choose two.)

A. User

B. Reporting Device

C. Failed-Logon Count

D. Event Type

E. Incident Identifier

ANSWER: A B

Explanation:

The baseline must maintain a separate behavioral history for each user and reporting-device combination. Therefore, **User** and **Reporting Device** are the appropriate Group By attributes. Failed-logon count is the value being measured, not a grouping dimension. Event Type should restrict the event population to failed logons, but it does not distinguish one user/device baseline from another.