PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7Security Operations 7.6 Architect

Fortinet NSE7_SOC_AR-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://passqueen.com

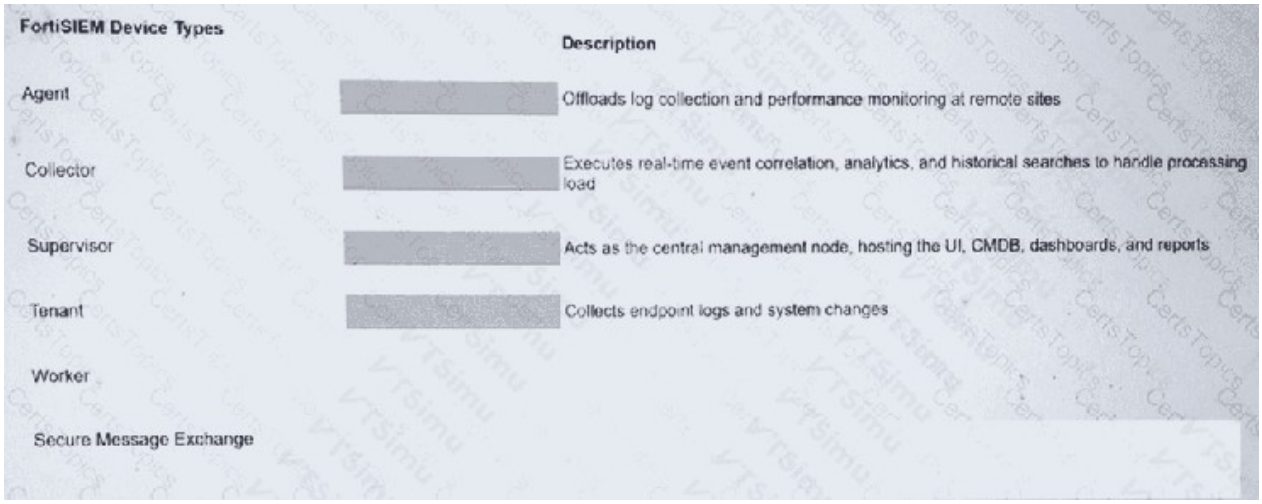
support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiAnalyzer	13
Topic 2, FortiSIEM	1
Topic 3, FortiSOAR	5
Topic 4, Mix Questions	4
Total	23

QUESTION NO: 1 - (SIMULATION)

Match the FortiSIEM device type to its description. Select each FortiSIEM device type in the left column, hold and drag it to the blank space next to its corresponding description in the column on the right.



ANSWER: See the explanation for the answer

Explanation:

Match the device types as follows:

Tenant and **Secure Message Exchange** are not used for these four descriptions.

QUESTION NO: 2

A SOC wants FortiAnalyzer to generate one high-priority event when the same source IP address produces failed VPN authentication attempts for five different user names within 10 minutes. Individual failed authentication logs must remain available for investigation but must not each create an incident. Which configuration best meets this requirement?

A. Configure an event handler with a failed-authentication filter and a threshold aggregated by source IP address

B. Configure a scheduled report that lists all failed VPN authentication events every 10 minutes

C. Forward each failed VPN authentication log to FortiSOAR and create an incident for every event

D. Add the VPN gateway address to an IOC list and generate an IOC event on every match

ANSWER: A

Explanation:

An event handler that filters failed VPN authentication events and applies a threshold with aggregation on the source IP address can identify the required pattern without generating an event for every individual failure. The original authentication logs remain stored and searchable in FortiAnalyzer for later investigation.

A scheduled report does not provide timely detection, and forwarding every failed log to FortiSOAR would create unnecessary alert volume before the correlation requirement has been met. An IOC match is not appropriate because the detection is based on authentication behavior rather than a known malicious indicator.