DUMPSARENA

Fortinet NSE 6OT Security 7.6 Architect

Fortinet NSE6_OTS_AR-7.6

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, OT Security Architecture	2
Topic 2, FortiGate	17
Topic 3, FortiNAC	1
Topic 4, FortiAnalyzer	2
Topic 5, Mix Questions	1
Total	23

QUESTION NO: 1

A legacy PLC cannot run an endpoint agent, but the access-layer switch connected to the PLC is manageable by FortiNAC. The plant wants to identify the device and restrict its network access if its observed behavior no longer matches its approved role. Which approach is the most appropriate?

A. Use FortiNAC agentless profiling with network access control through the managed switch.

B. Install a FortiNAC persistent agent on the PLC.

C. Use an IPS profile as the only method of identifying the PLC.

D. Assign the PLC a static MAC address in the FortiGate ARP table.

ANSWER: A

Explanation:

FortiNAC can perform agentless device discovery and profiling and can use supported network infrastructure to enforce access controls at the switch port. This approach is appropriate for OT devices, such as PLCs, that cannot support endpoint agents. Installing an endpoint agent is not feasible, while IPS inspection alone does not provide switch-port access control.

QUESTION NO: 2

FortiAnalyzer receives logs from FortiGate devices that protect OT zones. The security team requires an immediate notification when an IPS event matching a defined high-severity condition is logged. Which two FortiAnalyzer components are appropriate? (Choose two answers)

A. An event handler that filters for the required IPS event condition

B. A notification profile associated with the event handler

C. A scheduled report containing IPS statistics

D. A FortiManager policy package for the protected FortiGate devices

ANSWER: A B

Explanation:

An event handler can filter received logs for the required IPS event conditions and generate an alert when they match. A notification profile associated with the event handler delivers the alert through the configured notification method. A scheduled report is intended for periodic reporting rather than immediate alerting, and a FortiManager policy package does not process FortiAnalyzer log events.