PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 7 - Advanced Analytics 6.3

Fortinet NSE7_ADA-6.3

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 deployment and system configuration	1
Topic 2, FortiAnalyzer administration and management	1
Topic 3, FortiAnalyzer device management	1
Topic 4, Logging and report management	3
Topic 5, Event management	4
Topic 6, FortiSOC	13
Total	23

QUESTION NO: 1

A branch office contains network devices that can send syslog locally, but the service provider supervisor cannot directly reach the branch devices because of routing and firewall restrictions. The branch has reliable connectivity to the service provider FortiSIEM deployment.

Which deployment design is most appropriate?

A. Deploy a collector at the branch office and forward collected data to the FortiSIEM deployment.

B. Configure every branch device to be discovered directly by the supervisor.

C. Deploy a separate supervisor for each branch office.

D. Disable device discovery and collect only incident notifications.

ANSWER: A

Explanation:

A collector deployed at the branch can receive or collect data from local devices and forward it to the FortiSIEM deployment. This avoids requiring the supervisor to initiate direct connections to every branch device across the restricted network boundary. Sending all device logs directly to the supervisor would not address the stated reachability limitation for collection and discovery operations.

QUESTION NO: 2

What is the disadvantage of automatic remediation?

A. It can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network.

B. It is equivalent to running an IPS in monitor-only mode — watches but does not block.

C. External threats or attacks detected by FortiSIEM will need user interaction to take action on an already overworked SOC team.

D. Threat behaviors occurring during the night could take hours to respond to.

ANSWER: A

Explanation:

Automatic remediation can make a disruptive change to a user, block access to an application, or disconnect critical systems from the network. This is a key operational risk of allowing a security platform to execute a response without requiring an analyst's approval at the time of the event. For example, an automated playbook might quarantine an endpoint, disable an account, block a network connection, or change a firewall policy based on a detection. Although these actions can rapidly contain a genuine threat, an inaccurate detection, an incomplete understanding of the affected asset's role, or an overly broad response can interrupt legitimate business activity. The impact is particularly significant for sensitive systems and critical services, where isolating a device or denying access can affect users, applications, and dependent infrastructure. Effective use of automated remediation therefore requires carefully scoped actions, tested playbooks, reliable detection logic, and governance that accounts for business criticality. Fortinet describes its security operations and automation capabilities at FortiSIEM, and its broader automated-response approach at FortiSOAR.