Question #1 *Topic 1*

According to the National Institute of Standards and Technology (NIST) cybersecurity framework, incident handling activities can be divided into phases.
In which incident handling phase do you quarantine a compromised host in order to prevent an adversary from using it as a stepping stone to the next phase of an attack?

A. Containment

B. Recovery

C. Analysis

D. Eradication

Suggested Answer: *A*

Community vote distribution

A (100%)

Ati82 1 week, 1 day ago

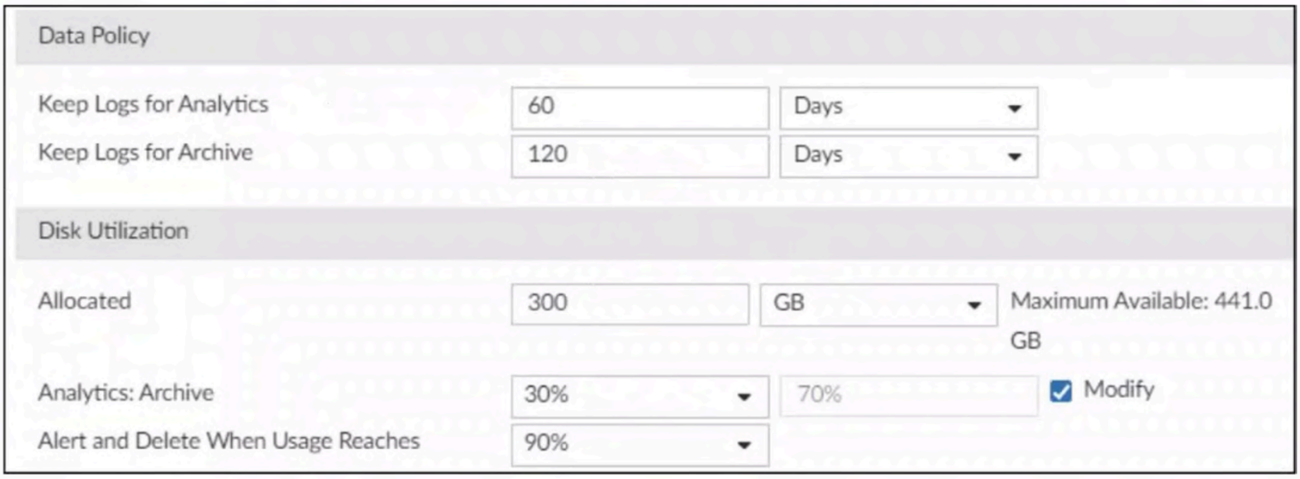
Selected Answer: A

https://www.bluevoyant.com/knowledge-center/nist-incident-response-framework-and-key-recommendations

upvoted 1 times

Question #2 *Topic 1*

Refer to the exhibit.



Data Policy

Keep Logs for Analytics 60 Days ▾

Keep Logs for Archive 120 Days ▾

Disk Utilization

Allocated 300 GB ▾ Maximum Available: 441.0 GB

Analytics: Archive 30% ▾ 70% ☑ Modify

Alert and Delete When Usage Reaches 90% ▾

You are tasked with reviewing a new FortiAnalyzer deployment in a network with multiple registered logging devices. There is only one FortiAnalyzer in the topology.

Which potential problem do you observe?

A. The archive retention period is too long.

B. The analytics-to-archive ratio is misconfigured.

C. The disk space allocated is insufficient.

D. The analytics retention period is too long.

Suggested Answer: *B*

Community vote distribution

B (100%)

Ati82 1 week, 1 day ago

Selected Answer: B

The defualt is 70:30

upvoted 1 times

Question #3 *Topic 1*

While monitoring your network, you discover that one FortiGate device is sending significantly more logs to FortiAnalyzer than all of the other FortiGate devices in the topology.
Additionally, the ADOM that the FortiGate devices are registered to consistently exceeds its quota.
What are two possible solutions? (Choose two.)

A. Reconfigure the first FortiGate device to reduce the number of logs it forwards to FortiAnalyzer.

B. Increase the storage space quota for the first FortiGate device.

C. Configure data selectors to filter the data sent by the first FortiGate device.

D. Create a separate ADOM for the first FortiGate device and configure a different set of storage policies.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Which role does a threat hunter play within a SOC?

A. Investigate and respond to a reported security incident

B. Monitor network logs to identify anomalous behavior

C. Collect evidence and determine the impact of a suspected attack

D. Search for hidden threats inside a network which may have eluded detection

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)

A. The supervisor uses an API to store logs, incidents, and events locally.

B. Downstream collectors can forward logs to Fabric members.

C. Logging devices must be registered to the supervisor.

D. Fabric members must be in analyzer mode.

Suggested Answer: *AD*

Community vote distribution

BD (100%)

⊟ **rakare** 1 month, 1 week ago

Selected Answer: BD

correct answer is bd

upvoted 1 times

⊟ **87be242** 2 months, 2 weeks ago

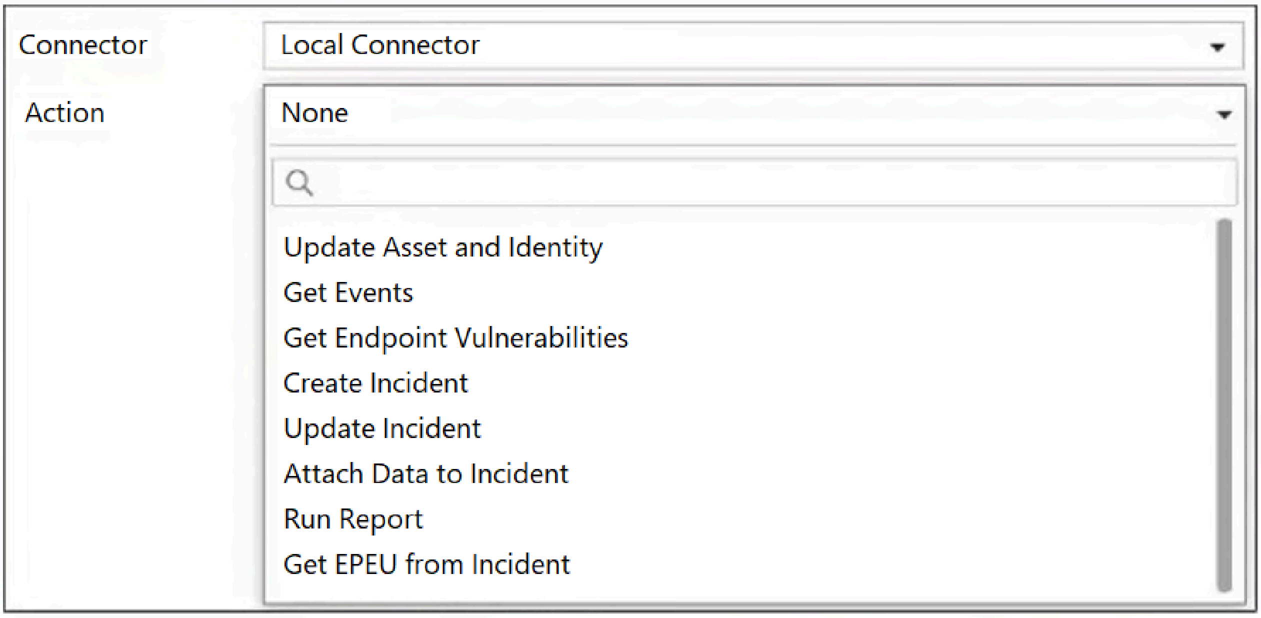
Selected Answer: BD

Study Guide p. 74-75

upvoted 1 times

Question #6 Topic 1

Refer to the exhibit.



A SOC analyst is designing a playbook to filter for a high severity event and attach the event information to an incident.

Which local connector action must the analyst use in this scenario?

A. Update Asset and Identity

B. Update Incident

C. Get Events

D. Attach Data to Incident

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

When does FortiAnalyzer generate an event?

A. When a log matches a filter in a data selector

B. When a log matches a rule in an event handler

C. When a log matches an action in a connector

D. When a log matches a task in a playbook

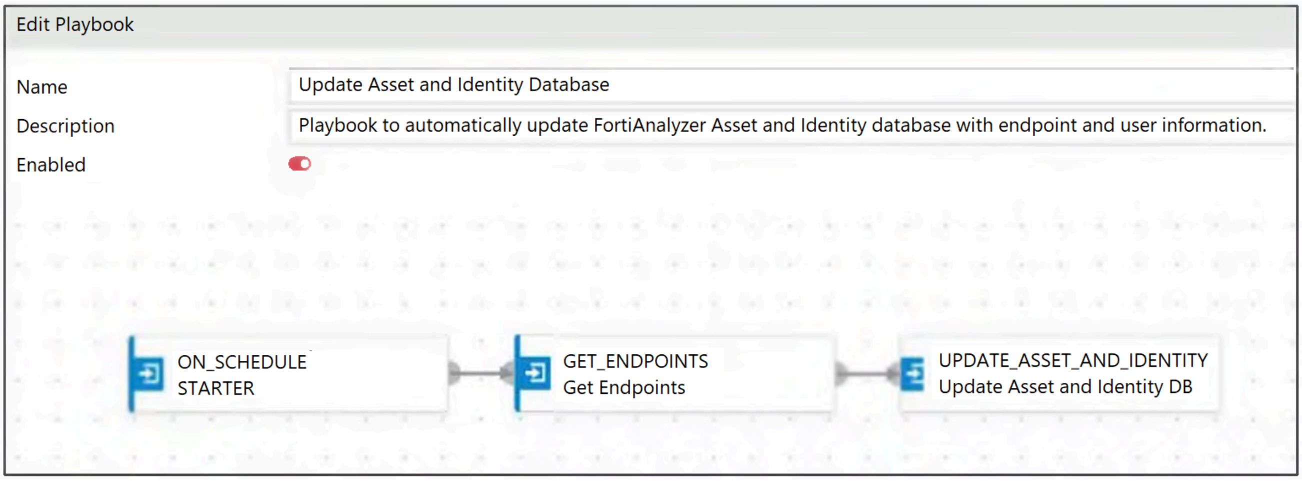
Suggested Answer: *B*

None

Question #8

Topic 1

Refer to the exhibit.



Edit Playbook

Name: Update Asset and Identity Database

Description: Playbook to automatically update FortiAnalyzer Asset and Identity database with endpoint and user information.

Enabled

Which two options describe how the Update Asset and Identity Database playbook is configured? (Choose two.)

A. The playbook is using a FortiMail connector.

B. The playbook is using a FortiClient EMS connector.

C. The playbook is using a local connector.

D. The playbook is using an on-demand trigger.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

When configuring a FortiAnalyzer to act as a collector device, which two steps must you perform? (Choose two.)

A. Configure Fabric authorization on the connecting interface.

B. Enable log compression.

C. Configure the data policy to focus on archiving.

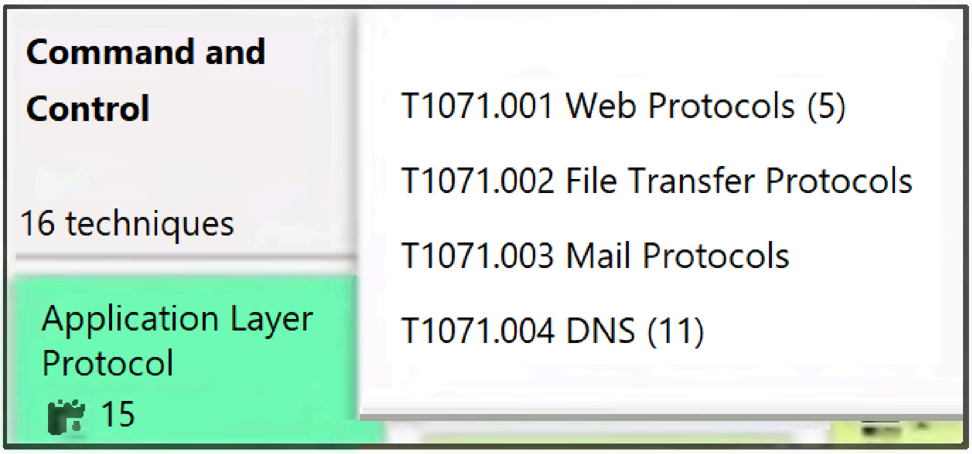
D. Configure log forwarding to a FortiAnalyzer in analyzer mode.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Refer to the exhibit, which shows the partial output of the MITRE ATT&CK Enterprise matrix on FortiAnalyzer.



Command and Control

16 techniques

Application Layer Protocol

15

T1071.001 Web Protocols (5)

T1071.002 File Transfer Protocols

T1071.003 Mail Protocols

T1071.004 DNS (11)

Which two statements are true? (Choose two.)

A. There are four techniques that fall under tactic T1071.

B. There are 15 events associated with the tactic.

C. There are four subtechniques that fall under technique T1071.

D. There are event handlers that cover tactic T1071.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Which FortiAnalyzer connector can you use to run automation stitches?

A. FortiCASB

B. FortiOS

C. FortiMail

D. Local

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which two playbook triggers enable the use of trigger events in later tasks as trigger variables? (Choose two.)

A. ON_DEMAND

B. ON_SCHEDULE

C. INCIDENT

D. EVENT

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Your company is doing a security audit. To pass the audit, you must take an inventory of all software and applications running on all Windows devices.
Which FortiAnalyzer connector must you use?

A. Local Host

B. FortiCASB

C. FortiClient EMS

D. ServiceNow

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!