Fortinet

FCSS_SOC_AN-7.4
FCSS - Security Operations 7.4 Analyst

For More Information – Visit link below:

https://www.examsboost.com/

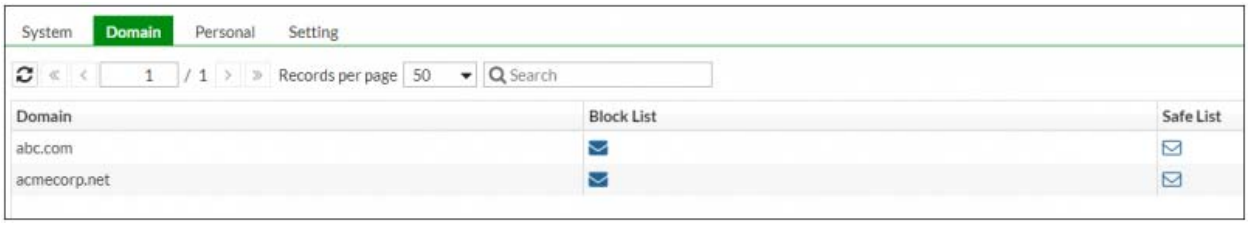
Product Version

✓ **Up to Date products, reliable and verified.**
✓ **Questions and Answers in PDF Format.**

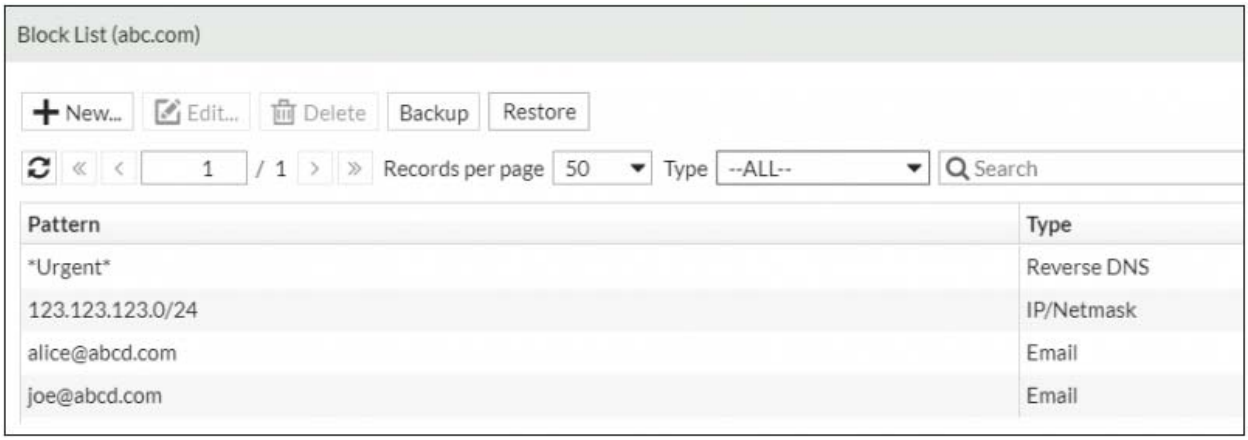
Latest Version: 6.0

Question: 1

Refer to the exhibits.
Domain List:



Domain abc.com:



Which connector and action on FortiAnalyzer can you use to add the entries show in the exhibits?
Response:

A. The FortiClient EMS connector and the quarantine action
B. The FortiMail connector and the add send to blocklist action
C. The Local connector and the update asset and identity action
D. The FortiMail connector and the get sender reputation action

Answer: B

Question: 2

Review the following incident report.

An unauthorized attempt to gain access to your network was detected. The attacker used a tool to identify system versions and services running on various ports.
The attacker likely used this information to exploit a known vulnerability on an outdated SSH server.
SSH server access attempts have been blocked, the server has been patched, and an investigation is underway to identify the attacker and assess the potential impact of the attack.

Which two MITRE ATT&CK tactics are captured in this report?
(Choose two.)
Response:

A. Defense Evasion
B. Priviledge Escalation
C. Reconnaissance
D. Execution

Answer: C,D

Question: 3

Which National Institute of Standards and Technology (NIST) incident handling phase involves removing malware and persistence mechanisms from a compromised host?
Response:

A. Eradication
B. Recovery
C. Containment
D. Analysis

Answer: A

Question: 4

You are tasked with configuring automation to quarantine infected endpoints. Which two Fortinet SOC components can work together to fulfill this task?
(Choose two.)
Response:

A. FortiAnalyzer
B. FortiClient EMS
C. FortiMail
D. FortiSandbox

Answer: A,B

Question: 5

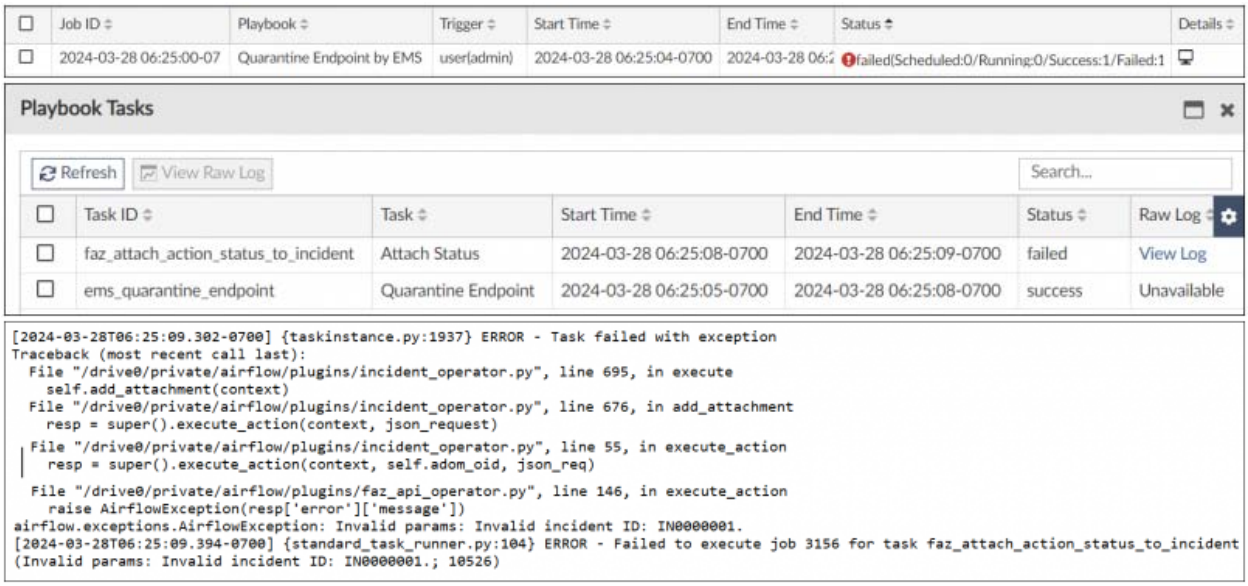
Which connector on FortiAnalyzer is responsible for looking up indicators to get threat intelligence?
Response:

A. The FortiGuard connector
B. The FortiOS connector
C. The FortiClient EMS connector
D. The local connector

Answer: A

Question: 6

Refer to the exhibits.



Job ID	Playbook	Trigger	Start Time	End Time	Status	Details
2024-03-28 06:25:00-07	Quarantine Endpoint by EMS	user(admin)	2024-03-28 06:25:04-0700	2024-03-28 06:2	failed(Scheduled:0/Running:0/Success:1/Failed:1	

Playbook Tasks

Refresh | View Raw Log | Search...

Task ID	Task	Start Time	End Time	Status	Raw Log
faz_attach_action_status_to_incident	Attach Status	2024-03-28 06:25:08-0700	2024-03-28 06:25:09-0700	failed	View Log
ems_quarantine_endpoint	Quarantine Endpoint	2024-03-28 06:25:05-0700	2024-03-28 06:25:08-0700	success	Unavailable

```
[2024-03-28T06:25:09.302-0700] {taskinstance.py:1937} ERROR - Task failed with exception
Traceback (most recent call last):
  File "/drive0/private/airflow/plugins/incident_operator.py", line 695, in execute
    self.add_attachment(context)
  File "/drive0/private/airflow/plugins/incident_operator.py", line 676, in add_attachment
    resp = super().execute_action(context, json_request)
  File "/drive0/private/airflow/plugins/incident_operator.py", line 55, in execute_action
    resp = super().execute_action(context, self.adom_oid, json_req)
  File "/drive0/private/airflow/plugins/faz_api_operator.py", line 146, in execute_action
    raise AirflowException(resp['error']['message'])
airflow.exceptions.AirflowException: Invalid params: Invalid incident ID: IN0000001.
[2024-03-28T06:25:09.394-0700] {standard_task_runner.py:104} ERROR - Failed to execute job 3156 for task faz_attach_action_status_to_incident
(Invalid params: Invalid incident ID: IN0000001.; 10526)
```

The Quarantine Endpoint by EMS playbook execution failed. What can you conclude from reviewing the playbook tasks and raw logs?
Response:

A. The playbook executed in an ADOM where the incident does not exist.
B. The admin user does not have the necessary rights to update incidents.
C. The local connector is incorrectly configured, which is causing JSON API errors.
D. The endpoint is quarantined, but the action status is not attached to the incident.

Answer: D

Question: 7

You are managing 10 FortiAnalyzer devices in a FortiAnalyzer Fabric. In this scenario, what is a benefit of configuring a Fabric group?
Response:

A. You can apply separate data storage policies per group.
B. You can aggregate and compress logging data for the devices in the group.
C. You can filter log search results based on the group.
D. You can configure separate logging rates per group.

Answer: C

Question: 8

You are not able to view any incidents or events on FortiAnalyzer. What is the cause of this issue?
Response:

A. FortiAnalyzer is operating in collector mode.
B. FortiAnalyzer is operating as a Fabric supervisor.
C. FortiAnalyzer must be in a Fabric ADOM.
D. There are no open security incidents and events.

Answer: A

Question: 9

Which FortiSASE component can be utilized for endpoint compliance?
Response:

A. Firewall-as-a-Service (FWaaS)
B. zero trust network access (ZTNA)
C. cloud access security broker (CASB)
D. secure web gateway (SWG)

Answer: B

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer