Boost up Your Certification Score

Fortinet

NSE7_SOC_AR-7.6

Fortinet NSE 7 - Security Operations 7.6 Architect

Exams Boost
Boost Up Your Career

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

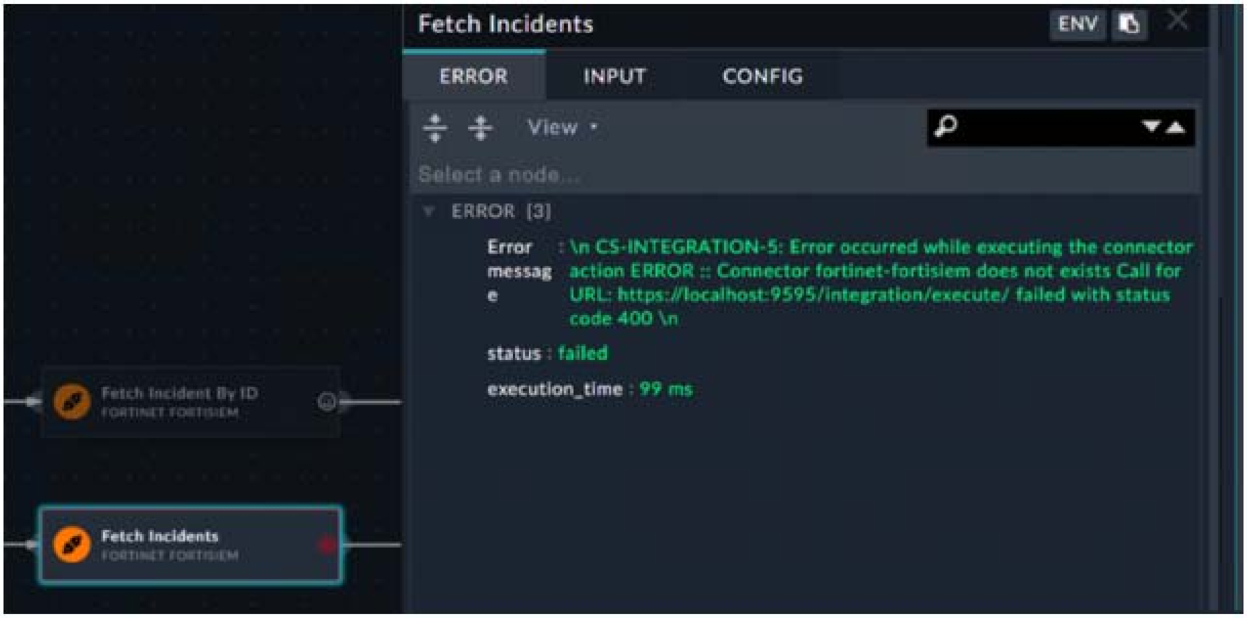
An administrator wants to detect if the CPU usage of a server exceeds 90% on average during a 10-minute window, at least twice. Which two aggregate conditions should you use together?
(Choose two.)

A. SUM(Matched Events)
B. COUNT(DISTINCT CPU Util)
C. AVG(CPU Util)
D. COUNT(Matched Events)

Answer: C,D

Question: 2

Refer to the exhibit.



```
ERROR [3]
    Error message : \n CS-INTEGRATION-5: Error occurred while executing the connector
                    action ERROR :: Connector fortinet-fortisiem does not exists Call for
                    URL: https://localhost:9595/integration/execute/ failed with status
                    code 400 \n
    status : failed
    execution_time : 99 ms
```

Based on the error message, where should you begin your troubleshooting?

A. Ensure the user has the Execute permission for the Playbooks module
B. Confirm that incidents matching your search criteria exist on FortiSIEM
C. Check the FortiSIEM connector configuration
D. Install the FortiSIEM connector from the content hub

Answer: C

Question: 3

What is the minimum number of FortiSIEM VMs required to collect event logs and generate incidents from matching rules?

A. 3
B. 2
C. 4
D. 1

Answer: D

Question: 4

Which FortiSOAR feature enables export and import of playbooks between environments (e.g., staging → production)?

A. Playbook Package Manager
B. Connector Library
C. Automation Center
D. System Diagnostics

Answer: A

Question: 5

Which three functions are supported by the data ingestion wizard in FortiSOAR?
(Choose three.)

A. Define a trigger to ingest data
B. Customize mapping of fields between the source system and FortiSOAR
C. Create separate data ingestion settings for each connector configuration
D. Choose between sequential, bulk, or parallel ingestion modes
E. Schedule data ingestion

Answer: B,C,E

Question: 6

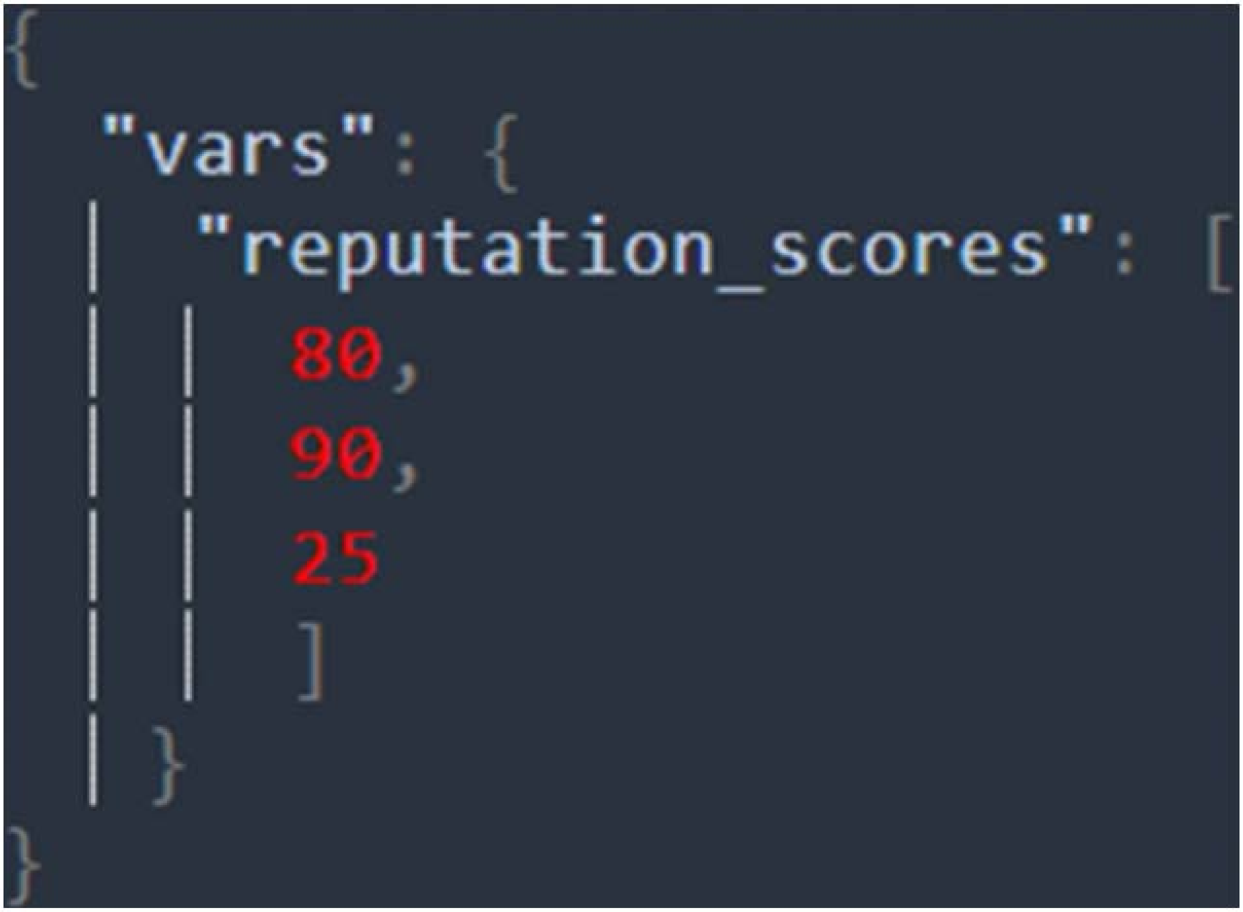
During threat hunting, an analyst filters logs by malicious IP and retrieves endpoint data from FortiClient EMS via API. Which FortiSOAR feature is used?

A. Connector Action Execution
B. Playbook Debugger
C. Report Designer
D. Incident Cloning

Answer: A

Question: 7

Refer to the exhibit.



```
{
  "vars": {
    "reputation_scores": [
      80,
      90,
      25
      ]
  }
}
```

Which Jinja expression will find the average of the three scores?

A. ((avg | vars.reputation_scores))
B. {{ (vars.reputation_scores | sum) / (vars.reputation_scores | length) }}
C. ((vars.reputation_scores.sum / length))
D. {{ sum(vars.reputation_scores) / length(vars.reputation_scores) }}

Answer: B

Question: 8

Which component controls how FortiSIEM distributes data collection load across multiple nodes?

A. Collector Group Assignment
B. Supervisor Scheduler
C. CMDB Indexing
D. Notification Policy

Answer: A

Question: 9

Which statement best describes the relationship between FortiSOAR and FortiSIEM in SOC operations?

A. FortiSOAR collects raw logs; FortiSIEM responds to incidents
B. FortiSIEM detects incidents; FortiSOAR automates response actions.
C. FortiSOAR correlates events; FortiSIEM manages queues.
D. They operate independently with no integration possible.

Answer: B

Question: 10

You want to configure a playbook step that meets the following requirements:
1. If the domain field contains corp-mail.example.com, it follows path A.
2. If the domain field contains malicious-badsite.net, it follows path B.
3. Otherwise, it follows a default path C.
Which type of playbook step allows you to implement this branching logic?

A. Manual Input
B. Loop
C. Decision
D. Connector

Answer: C

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

60 DAY MONEY BACK GUARANTEE 100% SATISFACTION GUARANTEED