Exam Questions NSE5_FSM-5.2

Fortinet NSE 5 - FortiSIEM 5.2

https://www.2passeasy.com/dumps/NSE5_FSM-5.2/

NEW QUESTION 1
A FortiSIEM administrator wants to restrict a network administrator to running searches for only firewall devices. Under role management, which option does the FortiSIEM administrator need to configure to achieve this scenario?

A. CMDB Report Conditions
B. Data Conditions
C. UI Access

Answer: B

NEW QUESTION 2
What is a prerequisite for FortiSIEM Linux agent installation?

A. The web server must be installed on the Linux server being monitored
B. The auditd service must be installed on the Linux server being monitored
C. The Linux agent manager server must be installed.
D. Both the web server and the audit service must be installed on the Linux server being monitored

Answer: D

NEW QUESTION 3
Refer to the exhibit.

How was the FortiGate device discovered by FortiSIEM?

A. Through GUI log discovery
B. Through syslog discovery
C. Using the pull events method
D. Through auto log discovery

Answer: A

NEW QUESTION 4
If a performance rule is triggered repeatedly due to high CPU use. what occurs m the incident table?

A. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.
B. The incident status changes to Repeated and the First Seen and Last Seen times are updated.
C. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated
D. The Incident Count value increases, and the First Seen and Last Seen tomes update

Answer: A

NEW QUESTION 5
Refer to the exhibit.

A FortiSIEM is continuously receiving syslog events from a FortiGate firewall The FortiSlfcM administrator is trying to search the raw event logs for the last two hours that contain the keyword tcp . However, the administrator is getting no results from the search.
Based on the selected filters shown in the exhibit, why are there no search results?

A. The keyword is case sensitive Instead of typing TCP in the Value fiel
B. the administrator should type tcp.
C. In the Time section, the administrator selected the Relative Last option, and in the drop-down lists, selected 2 and Hours as the lime period The time period should be 24 hours.
D. The administrator selected - in the Operator column That a the wrong operator.
E. The administrator selected AND in the Next drop-down lis
F. This is the wrong boolean operator.

Answer: C

NEW QUESTION 6
What are the four categories of incidents?

A. Devices, users, high risk, and low risk
B. Performance, availability, security, and change
C. Performance, devices, high risk, and low risk
D. Security, change, high risk, and low risk

Answer: B

NEW QUESTION 7
What operating system is FortiSIEM based on?

A. Cent OS
B. Microsoft Windows
C. RedHat
D. Ubuntu

Answer: A

NEW QUESTION 8
To determine whether or not syslog is being received from a network device, which is the best command from the backend?

A. tcpdump
B. phDeviceTest
C. netcat
D. phSyslogRecorder

Answer: A

NEW QUESTION 9
To determine SNMP discovery issues, which is the best command from the backend?

A. snmpwalk
B. phSNMPTest
C. snmptest
D. ssh

Answer: A

NEW QUESTION 10
In FotiSlEM enterprise licensing mode, if the link between the collector and data center FortiSlEM cluster a down what happens?

A. The collector drops incoming events like syslo
B. but slops performance collection
C. The collector continues performance collection of devices, but stops receiving syslog
D. The collector buffers events
E. The collector processes stop, and events are dropped

Answer: D

NEW QUESTION 10
If an incident’s status is Cleared, what does this mean?

A. Two hours have passed since the incident occurred and the incident has not reoccurred.
B. A clear condition set on a rule was satisfied.
C. A security rule issue has been resolved.
D. The incident was cleared by an operator.

Answer: B

NEW QUESTION 13
Which discovery scan type is prone to miss a device, if the device is quiet and the entry foe that device is not present in the ARP table of adjacent devices?

A. CMDB scan
B. L2 scan
C. Range scan
D. Smart scan

Answer: D

NEW QUESTION 17
Which two FortiSIEM components work together to provide real-time event correlation?

A. Collector and Windows agent
B. Supervisor and worker
C. Worker and collector
D. Supervisor and collector

Answer: D

NEW QUESTION 18
Refer to the exhibit.

If events are grouped by Event Receive Time, Reporting IP, and User attributes in FortiSIEM, how many results will be displayed?

A. Eight results will be displayed
B. Four results will be displayed
C. Two results will be displayed
D. Unique attributes cannot be grouped

Answer: D

NEW QUESTION 21
If the reported packet loss is between 50% and 98%. which status is assigned to the device in the Availability column of summary dashboard?

A. Down status is assigned because of packet loss.
B. Up status is assigned because of received packets
C. Critical status is assigned because of reduction in number of packets received
D. Degraded status is assigned because of packet loss

Answer: D

NEW QUESTION 26
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE5_FSM-5.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE5_FSM-5.2 Product From:

https://www.2passeasy.com/dumps/NSE5_FSM-5.2/

Money Back Guarantee

NSE5_FSM-5.2 Practice Exam Features:

* NSE5_FSM-5.2 Questions and Answers Updated Frequently

* NSE5_FSM-5.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE5_FSM-5.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE5_FSM-5.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year