NSE5_FSM-5.2 Q&As

Fortinet NSE 5 - FortiSIEM 5.2

Pass Fortinet NSE5_FSM-5.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse5_fsm-5-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.

An administrator is trying to identify an issue using an expression bated on the Expression Builder settings shown in the exhibit however, the error message shown in the exhibit indicates that the expression is invalid.

Which is the correct expression?

A. Matched Events COUNT()

B. Matched Events(COUNT)

C. COUNT(Matched Events)

D. (COUNT) Matched Events

Correct Answer: C

QUESTION 2

What is the best discovery scan option for a network environment where ping is disabled on all network devices?

A. Smart scan

B. Range scan

C. CMDB scan

D. L2 scan

Correct Answer: A

QUESTION 3

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

Correct Answer: B

QUESTION 4

What protocol can be used to collect Windows event logs in an agentless method?

A. SSH

B. SNMP

C. WMI

D. SMTP

Correct Answer: C

QUESTION 5

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

Correct Answer: B

NSE5_FSM-5.2 Practice Test NSE5_FSM-5.2 Study Guide NSE5_FSM-5.2 Braindumps