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.passapply.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)

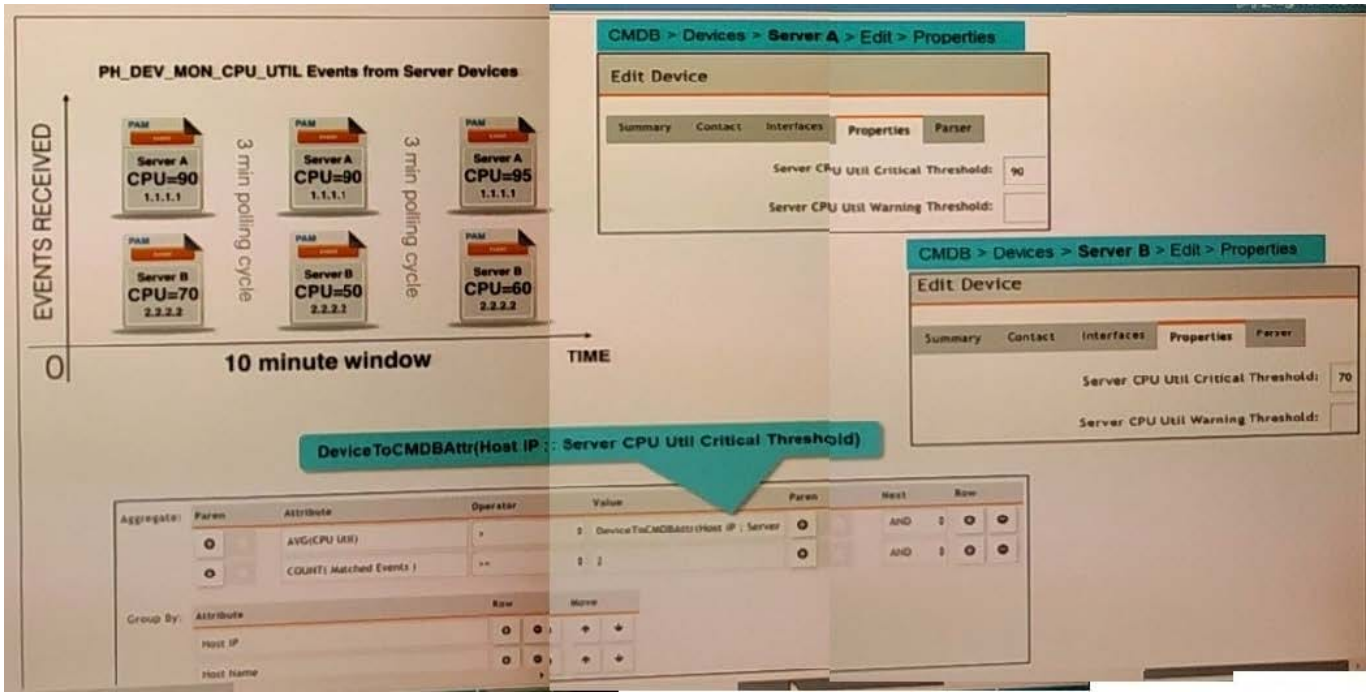
C. COUNT(Matched Events)

D. (COUNT) Matched Events

Correct Answer: C

QUESTION 2

Refer to the exhibit.



Three events are collected over a 10-minutc time period from two servers Server A and Server B. Based on the settings being used for the rule subpattern. how many incidents will the servers generate?

A. Server A will not generate any incidents and Server B will not generate any incidents

B. Server A will generate one incident and Server B wifl generate one incident

C. Server A will generate one incident and Server B will not generate any incidents

D. Server B will generate one incident and Server A will not generate any incidents

Correct Answer: A

QUESTION 3

In the rules engine, which condition instructs FortiSIEM to summarize and count the matching evaluated data?

A. Time Window

B. Aggregation

C. Group By

D. Filters

Correct Answer: C

QUESTION 4

What operating system is FortiSIEM based on?

A. Cent OS

B. Microsoft Windows

C. RedHat

D. Ubuntu

Correct Answer: A

QUESTION 5

Which two export methods are available for FortiSIEM analytics results? (Choose two.)

A. CSV

B. PNG

C. HTML

D. PDF

Correct Answer: AD