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

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

Correct Answer: A

QUESTION 2

Refer to the exhibit.
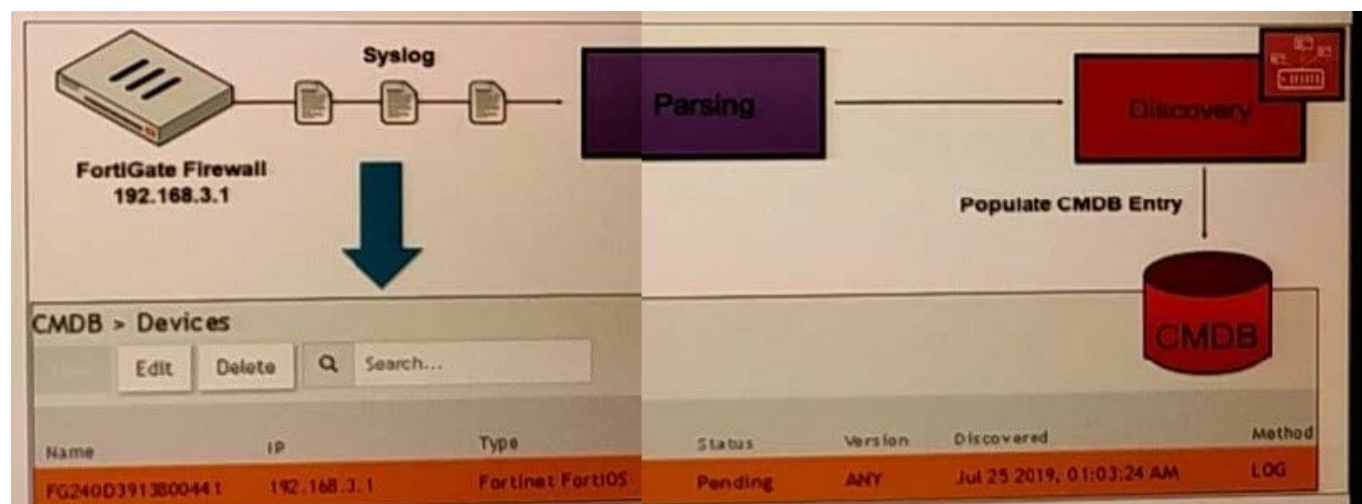
How was the FortiGate device discovered by FortiSIEM?

A. Through GUI log discovery

B. Through syslog discovery

C. Using the pull events method

D. Through auto log discovery

Correct Answer: A

QUESTION 3

Which process convertsRaw log data to structured data?

A. Data enrichment

B. Data classification

C. Data parsing

D. Data validation

Correct Answer: D

QUESTION 4

A FortiSIEM supervisor at headquarters is struggling to keep up with an increase of EPS (Events Per Second) being reported across the enterprise. What components should an administrator consider deploying to assist the supervisor with processing data?

A. Supervisor

B. Worker

C. Collector

D. Agent

Correct Answer: B

QUESTION 5

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

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

A. Seven results will be displayed.

B. There results will be displayed.

C. Unique attribute cannot be grouped.

D. Five results will be displayed.

Correct Answer: D

NSE5_FSM-5.2 PDF Dumps

NSE5_FSM-5.2 VCE Dumps

NSE5_FSM-5.2 Practice Test