Fortinet

Exam Questions FCP_FSM_AN-7.2

FCP - FortiSIEM 7.2 Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

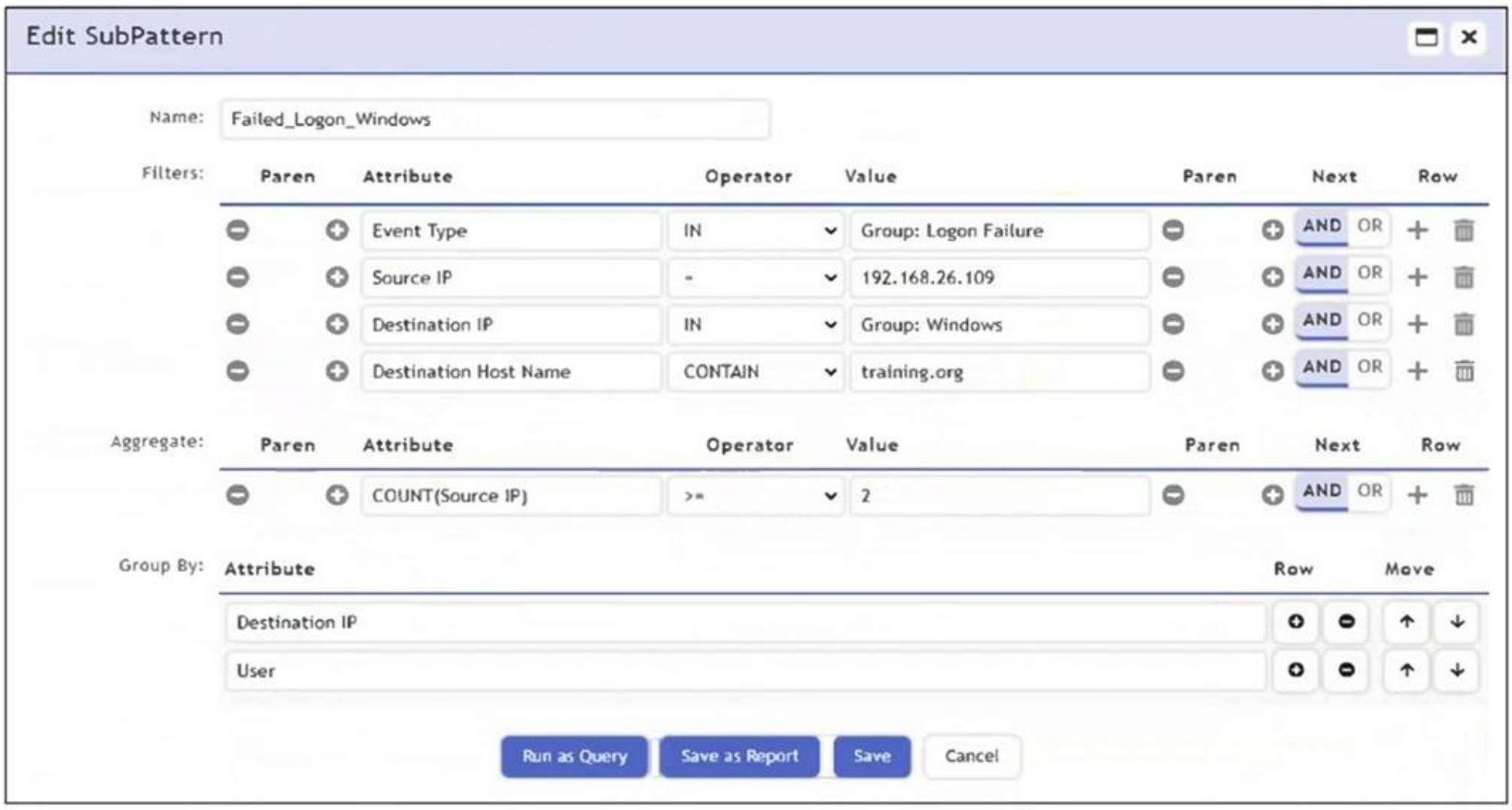
Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.

SubPattern edit window



An analyst is troubleshooting the rule shown in the exhibit. It is not generating any incidents, but the filter parameters are generating events on the Analytics tab. What is wrong with the rule conditions?

A. The Event Type refers to a CMDB lookup and should be an Event lookup.
B. The Destination Host Name value is not fully qualified.
C. The Group By attributes restricts which events are counted.
D. The Aggregate attribute is too restrictive.

Answer: C

NEW QUESTION 2
Refer to the exhibit.

Event Attribute

A FortiSIEM device is receiving syslog events from a FortiGate firewall. The FortiSIEM analyst is trying to search the raw event logs for the last two hours that contain the keyword "udp". However, they are getting no results from the search, which they know should be available. Based on the filter shown in the exhibit, why

are there no search results?

A. The analyst selected AND in the Next colum
B. This is the wrong Boolean operator.
C. The Time Range value should be set to Real-Time.
D. The keyword is case sensitiv
E. Instead of typing udp in the Value field, the analyst should type UDP.
F. The analyst selected = in the Operator colum
G. That is the wrong operator.

Answer: D

NEW QUESTION 3
What are two required components of a rule? (Choose two.)

A. Exception policy
B. Subpattern
C. Detection Technology
D. Clear policy

Answer: BC

NEW QUESTION 4
Which information can FortiSIEM retrieve from FortiClient EMS through an API connection?

A. Host software versions
B. FortiSIEM license
C. Host login credentials
D. ZTNA tags

Answer: D

Explanation:
FortiSIEM can retrieve ZTNA tags from FortiClient EMS through an API connection, enabling dynamic user and device classification for policy enforcement and incident response.

NEW QUESTION 5
Which two settings must you configure to allow FortiSIEM to apply tags to devices in FortiClient EMS? (Choose two.)

A. FortiEMS API credentials defined on FortiSIEM
B. Remediation script configured
C. ZTNA tags defined on FortiSIEM
D. FortiSIEM API credentials defined on FortiEMS\

Answer: AC

NEW QUESTION 6
Refer to the exhibit.

What is the Group: FortiSIEM Analysts value referring to?

A. FortiSIEM organization group
B. LDAP user group

C. CMDB user group
D. Windows Active Directory user group

Answer: C

NEW QUESTION 7
Which running mode takes the most time to perform machine learning tasks?

A. Local auto
B. Local
C. Forecasting
D. Regression

Answer: A

NEW QUESTION 10
.....

Relate Links

100% Pass Your FCP_FSM_AN-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FSM_AN-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/