



Vendor: Fortinet

Exam Code: FCP_FSM_AN-7.2

Exam Name: FCP - FortiSIEM 7.2 Analyst

Version: DEMO

QUESTION 1

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: AD

Explanation:

To allow FortiSIEM to apply tags to devices in FortiClient EMS, FortiEMS API credentials must be defined on FortiSIEM to enable communication with EMS, and FortiSIEM API credentials must be defined on FortiEMS to allow EMS to accept tagging instructions from FortiSIEM. This bidirectional API trust is essential for tag application.

QUESTION 2

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

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

Answer: BC

Explanation:

A Subpattern defines the specific conditions or event patterns the rule is designed to detect, and the Detection Technology specifies the type of detection logic (e.g., real-time, historical). Both are essential for a rule to function in FortiSIEM.

QUESTION 3

What can you use to send data to FortiSIEM for user and entity behavior analytics (UEBA)?

- A. FortiSIEM agent
- B. SSH
- C. SNMP
- D. FortiSIEM worker

Answer: A

Explanation:

The FortiSIEM agent can be used to send detailed endpoint data such as user activity and process behavior to FortiSIEM, which is essential for performing User and Entity Behavior Analytics (UEBA).

QUESTION 4

Which items are used to define a subpattern?

- A. Filters, Aggregate, Group By definitions
- B. Filters, Aggregate, Time Window definitions
- C. Filters, Group By, Threshold definitions

D. Filters, Threshold, Time Window definitions

Answer: A

Explanation:

A subpattern in FortiSIEM is defined using Filters to match specific events, Aggregate conditions to apply statistical thresholds (e.g., COUNT), and Group By attributes to segment data for evaluation. These three components collectively determine how the subpattern functions.

QUESTION 5

How can you query the configuration management database (CMDB) in an analytics search?

- A. Click Value > Select from CMDB.
- B. On the CMDB tab, select an entry, and then click Create Search.
- C. On the Admin tab, click CMDB Search.
- D. Click Attribute > Select from CMDB.

Answer: A

Explanation:

In an analytics search, you can query the CMDB by clicking Value > Select from CMDB, which allows you to choose values directly from CMDB entries for the selected attribute, enabling precise filtering based on asset data.

QUESTION 6

When configuring anomaly detection machine learning, in which step must you select the fields to analyze?

- A. Design
- B. Schedule
- C. Prepare Data
- D. Train

Answer: C

Explanation:

In the Prepare Data step of configuring anomaly detection in FortiSIEM, you must select the fields to analyze. This step defines the input features that the machine learning model will evaluate during training and detection.

QUESTION 7

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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14