

Fortinet FCP_FSM_AN-7.2 Cert & Exam

FCP_FSM_AN-7.2 Tips



P.S. Free & New FCP_FSM_AN-7.2 dumps are available on Google Drive shared by Pass4Test: <https://drive.google.com/open?id=1znPeLj1fF5mN3nxEgC7TuyCLsLzQThm>

The world is a stage. We must seize all opportunities for career progression and to actualize our dream. So, you must seize Pass4Test to undersell yourself in the future. Pass4Test Fortinet FCP_FSM_AN-7.2 study guide will help you to overcome difficulties and to get the certification. We will help you to understand the laws of FCP_FSM_AN-7.2 Exam. Pass4Test provides original questions and pdf real questions and answers. If you get the certification, you will rise to undreamed-of heights.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	Analytics: This section of the exam measures the skills of Security Analysts and covers the foundational techniques for building and refining queries. It focuses on creating searches from events, applying grouping and aggregation methods, and performing various lookup operations, including CMDB and nested queries to effectively analyze and correlate data.
Topic 2	Rules and subpatterns: This section of the exam measures the skills of SOC Engineers and focuses on the construction and implementation of analytics rules. It involves identifying the different components that make up a rule, utilizing advanced features like subpatterns and aggregation, and practically configuring these rules within the FortiSIEM platform to detect security events.
Topic 3	Incidents, notifications, and remediation: This section of the exam measures the skills of Incident Responders and encompasses the entire incident management lifecycle. This includes the skills required to manage and prioritize security incidents, configure policies for alert notifications, and set up automated remediation actions to contain and resolve threats.

Topic 4	Machine learning, UEBA, and ZTNA: This section of the exam measures the skills of Advanced Security Architects and covers the integration of modern security technologies. It involves performing configuration tasks for machine learning models, incorporating UEBA (User and Entity Behavior Analytics) data into rules and dashboards for enhanced threat detection, and understanding how to integrate ZTNA (Zero Trust Network Access) principles into security operations.
---------	---

>> Fortinet FCP_FSM_AN-7.2 Cert <<

Exam FCP_FSM_AN-7.2 Tips, FCP_FSM_AN-7.2 Useful Dumps

The three versions of our FCP_FSM_AN-7.2 practice braindumps have their own unique characteristics. The PDF version of FCP_FSM_AN-7.2 training materials is convenient for you to print, the software version of training guide can provide practice test for you and the online version is for you to read anywhere at any time. If you are hesitating about which version should you choose, you can download our FCP_FSM_AN-7.2 free demo first to get a firsthand experience before you make any decision.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q17-Q22):

NEW QUESTION # 17

Refer to the exhibit.



Which value would you expect the FortiSIEM parser to use to populate the Application Name field?

- A. SSL
- B. wan1
- C. applist
- D. Network.Service

Answer: A

Explanation:

The Application Name field in FortiSIEM is typically populated using the value of the app field in the raw log. In this event, app="SSL", so "SSL" is the expected application name parsed by FortiSIEM.

NEW QUESTION # 18

Refer to the exhibit.

Incident Details



Server Disk Latency C:\ Critical on THREATSOCDC



Actions

Search...

Incident ID : 3984

Incident Title : Server Disk Latency C:\ Critical on THREATSOCDC

Rule Name : Server Disk Latency Critical

Event Type : PH_RULE_SERVER_DISK_LATENCY_CRIT

Severity Category : **High**

First Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Last Occurred : 33 Minutes ago (Jan 15 2025, 08:07:15 AM)

Category : Performance

Subcategory : Impact

Tactics : Impact

Technique : Endpoint Denial of Service: OS Exhaustion Flood

Organization : Super

Reporting : **30** WIN-RAQBSNW8OVY

Reporting IP : **30** 10.1.1.33

Reporting Device Status : Pending

Target : **30** 10.1.1.33

THREATSOCDC

Detail : Disk Name: C:\

Disk Read Latency ms: 100.03ms

Disk Write Latency ms: 1ms

Count : 1

Incident Status : Auto Cleared

Cleared Reason : Rule has not been triggered for 20 minutes

Cleared Time : 13 Minutes ago (Jan 15 2025, 08:27:17 AM)

How was this incident cleared?

- A. FortiSIEM cleared the incident automatically after 24 hours.
- **B. The incident was cleared automatically by the rule.**
- C. The analyst manually cleared the incident from the incident table.
- D. The endpoint was rebooted and sent an all-clear signal to FortiSIEM.

Answer: B

Explanation:

The Incident Status shows "Auto Cleared", and the Cleared Reason states: "Rule has not been triggered for 20 minutes." This indicates that the incident was automatically cleared by the rule logic after a defined period of inactivity.

NEW QUESTION # 19

Refer to the exhibit.

Subpattern 1

Edit SubPattern

Name: RDP_Connection

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Destination TCR/UDP Port	=	3389	-	AND OR	+
	+	Event Type	=	FortiGate-traffic-forward	-	AND OR	+

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	COUNT(Matched Events)	>=	1	-	AND OR	+

Group By: Attribute

Attribute	Row	Move
User	○ ○	↑ ↓
Source IP	○ ○	↑ ↓

Run as Query Save as Report Save Cancel

Subpattern 2

Edit SubPattern

Name: Failed_Logon

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	Event Type	IN	Group: Logon Failure	-	AND OR	+

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	+	COUNT(Matched Events)	>=	3	-	AND OR	+

Group By: Attribute

Attribute	Row	Move
User	○ ○	↑ ↓
Source IP	○ ○	↑ ↓
Destination IP	○ ○	↑ ↓

Run as Query Save as Report Save Cancel

Rule Conditions

Step 1: General > **Step 2: Define Condition** > Step 3: Define Action

Condition: If this Pattern occurs within any 300 second time window

Paren	Subpattern	Paren	Next	Row
○ ○	RDP_Connection	○ ○	FOLLOWED_BY	○ ○
○ ○	Failed_Logon	○ ○		○ ○

Given these Subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next	Row
RDP_Connection	User	=	Failed_Logon	User	AND	○ ○
RDP_Connection	Source IP	=	Failed_Logon	Source IP		○ ○

Save Cancel

Which two conditions will match this rule and subpatterns? (Choose two.)

- A. A user connects to the wrong IP address for an RDP session five times.
- B. A user fails twice to log in when connecting through RDP.
- C. A user runs a brute force password cracker against an RDP server.
- D. A user using RDP over SSL VPN fails to log in to an application five times.

Answer: C,D

Explanation:

The user initiates an RDP session (Subpattern 1) and then fails to log in multiple times (Subpattern 2 with COUNT(Matched Events) >= 3) - both from the same Source IP and User within 300 seconds.

The brute force attempts typically involve a successful RDP connection followed by multiple failed logins, satisfying the sequence and grouping conditions in the rule.

NEW QUESTION # 20

Which analytics search can be used to apply a user and entity behavior analytics (UEBA) tag to an event for a failed login by the user JSmith?

- A. User IS jsmith
- B. Username CONTAIN smit
- C. User = smith
- D. Username NOT END WITH jsmith

Answer: A

Explanation:

The correct syntax to match an exact username in FortiSIEM analytics search is User IS jsmith. This ensures that the UEBA tag is applied only when the event is specifically tied to the user "jsmith", which is required for accurate behavioral analytics.

NEW QUESTION # 21

Refer to the exhibit.

The screenshot shows the 'Machine Learning - Train Configuration' window in FortiSIEM. It includes a 'Run Mode' dropdown set to 'Local', a 'Task' dropdown set to 'Regression', and an 'Algorithm' dropdown set to 'DecisionTreeRegressor'. Below these is a section titled 'Fields to use for Prediction:' which contains a list of fields with checkboxes. The fields are: 'AVG(CPU Util)' (unchecked), 'AVG(Memory Util)' (checked), 'AVG(Sent Bytes64)' (checked), and 'AVG(Received Bytes64)' (checked). A large 'FORTINET' watermark is visible across the right side of the interface, and a 's4test.com' watermark is visible at the bottom.

Machine Learning - Train Configuration

▶ Run Mode: Local

▶ Task: Regression

▶ Algorithm: DecisionTreeRegressor

▼ Fields to use for Prediction:

- ☐ AVG(CPU Util)
- ☒ AVG(Memory Util)
- ☒ AVG(Sent Bytes64)
- ☒ AVG(Received Bytes64)

The screenshot shows a configuration window for FortiSIEM. Under the 'Field to Predict' section, 'AVG(CPU Util)' is selected with a radio button. Below it, 'AVG(Memory Util)', 'AVG(Sent Bytes64)', and 'AVG(Received Bytes64)' are listed but are disabled (grayed out). In the 'Train factor' section, there is a slider bar ranging from 0% to 100%. The slider is currently positioned at approximately 30%, and the value '30' is displayed in a text box to the right of the slider.

The configuration shown in the exhibit is incorrect.

What must you change to allow this configuration to be successfully applied to FortiSIEM?

- A. The Train factor must be 70% or greater.
- B. The selection in Fields to use for Prediction and Field to Predict must match.
- C. Run Mode must be set to ML.
- D. Only one AVG type field must be selected under Fields to use for Prediction.

Answer: C

Explanation:

The Run Mode is set to Local, which is not valid for training machine learning models in FortiSIEM. To apply this configuration correctly, the Run Mode must be set to ML, which enables proper model training and prediction using selected fields.

NEW QUESTION # 22

.....

If you want to pass a high percentage of the Fortinet FCP_FSM_AN-7.2 Exam, you should consider studying for the actual exam. These practice tests are designed to help you prepare for the exam and ensure you know the syllabus content. It will also help you improve your time management skills, as these tests are designed like an actual exam. Moreover, they will help you learn to answer all questions in the time allowed.

Exam FCP_FSM_AN-7.2 Tips: https://www.pass4test.com/FCP_FSM_AN-7.2.html

- Free FCP_FSM_AN-7.2 Brain Dumps □ FCP_FSM_AN-7.2 Latest Exam Dumps □ Exam FCP_FSM_AN-7.2 Braindumps □ Go to website ✨ www.examcollectionpass.com □ ✨ □ open and search for ► FCP_FSM_AN-7.2 ◀ to download for free □ FCP_FSM_AN-7.2 Test Dumps
- Valid Exam FCP_FSM_AN-7.2 Book □ Exam FCP_FSM_AN-7.2 Braindumps □ Study FCP_FSM_AN-7.2 Plan ♥ Open □ www.pdfvce.com □ and search for (FCP_FSM_AN-7.2) to download exam materials for free □ Exam FCP_FSM_AN-7.2 Braindumps
- FCP_FSM_AN-7.2 Pass4sure Study Materials □ Books FCP_FSM_AN-7.2 PDF □ Exam FCP_FSM_AN-7.2 Braindumps □ Enter (www.prep4sures.top) and search for { FCP_FSM_AN-7.2 } to download for free ☎ Study FCP_FSM_AN-7.2 Plan

- [illegible]

P.S. Free 2026 Fortinet FCP_FSM_AN-7.2 dumps are available on Google Drive shared by Pass4Test: <https://drive.google.com/open?id=1znPeLj1fF5mN3nxEGC7TuyvLsLzOThm>