

FCP_FSM_AN-7.2 Valid Mock Test - Free

FCP_FSM_AN-7.2 Pdf Guide

Subpattern 1

Edit SubPattern

Name: RDP_Connection

Filters	Param	Attribute	Operator	Value	Param	Next	Row
☒	Expiration	ICM-ICM-Port	=	328	☒	AND	OK
☒	Event Type		=	FortiGate-traffic-forward	☒	AND	OK

Aggregates	Param	Attribute	Operator	Value	Param	Next	Row
☒	COUNT (matched Events)		>=	1	☒	AND	OK

Group By: Attribute

Row	Move
User	☐ ☐ ☐ ☐
Source IP	☐ ☐ ☐ ☐

Buttons: Run as Query, Save as Report, Save, Cancel

Subpattern 2

Edit SubPattern

Name: Failed_Login

Filters	Param	Attribute	Operator	Value	Param	Next	Row
☒	Event Type		is	Group: Login Failure	☒	AND	OK

Aggregates	Param	Attribute	Operator	Value	Param	Next	Row
☒	COUNT (matched Events)		>=	1	☒	AND	OK

Group By: Attribute

Row	Move
User	☐ ☐ ☐ ☐
Source IP	☐ ☐ ☐ ☐
Destination IP	☐ ☐ ☐ ☐

Buttons: 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

Param	Subpattern	Param	Next	Row
☒	RDP_Connection	☒	FOLLOWED_BY	☒
☒	Failed_Login	☒		☒

Given these Subpattern relationships:

Subpattern	Attribute	Operator	Subpattern	Attribute	Next	Row
RDP_Connection	User	=	Failed_Login	User	AND	☒
RDP_Connection	Source IP	=	Failed_Login	Source IP		☒

Buttons: Save, Cancel

2026 Latest ITExamSimulator FCP_FSM_AN-7.2 PDF Dumps and FCP_FSM_AN-7.2 Exam Engine Free Share:
https://drive.google.com/open?id=1C8W_tx45eLav0jkytU6_KCHTsaPgFKP4

With FCP_FSM_AN-7.2 test training materials of ITExamSimulator, you can put away with disorder emotion and clean up them. FCP_FSM_AN-7.2 test training materials of ITExamSimulator are the most accurate training materials in the current market. Using it, the passing rate of FCP_FSM_AN-7.2 Exam is 100%. Choose ITExamSimulator is equal to choose success.

Fortinet FCP_FSM_AN-7.2 Exam Overview:

Certification Vendor:	Fortinet
Exam Name:	FCP - FortiSIEM 7.2 Analyst
Exam Number:	FCP_FSM_AN-7.2
Certificate Validity Period:	2 years
Exam Format:	Multiple Choice, Multiple Select
Exam Price:	USD 400
Real Exam Qty:	35
Exam Duration:	120 minutes
Passing Score:	60%
Related Certifications:	FCP - FortiSIEM

Available Languages:	English
Sample Questions:	Fortinet FCP_FSM_AN-7.2 Sample Questions
Exam Way:	Online proctored or at Pearson VUE testing center
Pre Condition:	Recommended: FortiSAE, FortiSIEM training courses or equivalent practical experience
Official Syllabus URL:	https://www.fortinet.com/training/certification

>> **FCP_FSM_AN-7.2 Valid Mock Test** <<

Latest FCP_FSM_AN-7.2 Exam Torrent Must Be a Great Beginning to Prepare for Your Exam - ITExamSimulator

With all types of FCP_FSM_AN-7.2 test guide selling in the market, lots of people might be confused about which one to choose. Many people can't tell what kind of FCP_FSM_AN-7.2 study dumps and software are the most suitable for them. Our company can guarantee that our FCP_FSM_AN-7.2 Actual Questions are the most reliable. Having gone through about 10 years' development, we still pay effort to develop high quality FCP_FSM_AN-7.2 study dumps and be patient with all of our customers, therefore you can trust us completely.

Fortinet FCP_FSM_AN-7.2 Exam Syllabus Topics:

Topic	Details
Topic 1	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 2	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 3	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.
Topic 4	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.

Fortinet FCP - FortiSIEM 7.2 Analyst Sample Questions (Q11-Q16):

NEW QUESTION # 11

Refer to the exhibits.

Subpattern 1



Edit SubPattern

Name: RDP_Connection

Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
+	+	Destination TCP/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	-	OR	+
+	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	AND	+

Save Cancel

An analyst is troubleshooting why the rule shown in the exhibit is generating incidents for successful RDP connections. Given the rule conditions and subpatterns, what is causing the problem?

- A. The Failed_Logon subpattern is not checking for failed authentications.
- B. The subpattern relationship RDP_Connection:User = Failed_Logon:User will never match.
- C. The condition time window is too short.
- D. The Boolean between the subpatterns is incorrect.

Answer: D

Explanation:

The rule condition combines the two subpatterns with an OR, so the rule fires when either an RDP_Connection event or a

Failed_Logon pattern occurs. This causes incidents to be generated for successful RDP connections even when no failed logons are present. The subpatterns should be combined with AND so that incidents are created only when both the RDP connection and the failed logons occur together.

NEW QUESTION # 12

Refer to the exhibit.

Machine Learning - Train Configuration

The image shows a configuration window for Machine Learning training. It has several sections:

- Run Mode:** Local
- Task:** Regression
- Algorithm:** DecisionTreeRegressor
- Fields to use for Prediction:** A list of fields with checkboxes. ☐ AVG(CPU Util), ☒ AVG(Memory Util), ☒ AVG(Sent Bytes64), ☒ AVG(Received Bytes64).
- Field to Predict:** A list of fields with radio buttons. ☒ AVG(CPU Util), ☐ AVG(Memory Util), ☐ AVG(Sent Bytes64), ☐ AVG(Received Bytes64).
- Train factor:** A slider from 0% to 100% with a value of 30.

A watermark "itexamsimulator.com" is visible across the center. The Fortinet logo is in the bottom right corner.

The configuration shown in the exhibit is incorrect.

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

- A. The selection in Fields to use for Prediction and Field to Predict must match.
- B. Run Mode must be set to ML.

- C. Only one AVG type field must be selected under Fields to use for Prediction.
- D. The Train factor must be 70% or greater.

Answer: B

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 # 13

Which two data areas can you use for user and entity behavior analytics (UEBA) machine learning models? (Choose two.)

- A. network
- B. process
- C. resources
- D. location

Answer: A,D

Explanation:

FortiSIEM's UEBA models analyze user and entity behavior by correlating data such as location (for detecting unusual logins or access patterns) and network activity (for identifying abnormal communication or traffic behaviors). These data areas enable the system to build baseline profiles and detect anomalies indicating potential insider threats or compromised accounts.

NEW QUESTION # 14

Refer to the exhibit.

Source IP	Reporting Device	Reporting IP	Event Type	User	Count
15.2.3.4	FW01	10.1.1.1	Logon	Mike	4
21.3.4.5	FW01	10.1.1.1	Logon	Bob	3
14.12.3.1	FW01	10.1.1.1	Logon	Alice	2
192.168.1.5	FW01	10.1.1.1	Logon	Alice	2
10.1.1.1	FW01	10.1.1.1	Logon	Bob	6
123.123.1.1	FW01	10.1.1.1	Logon	Mike	5

If you group the events by User and Count attributes, how many results will FortiSIEM display?

- A. Three
- B. Six
- C. Five
- D. One
- E. Two

Answer: C

Explanation:

Grouping by User and Count yields five unique pairs: (Mike,4), (Bob,3), (Alice,2), (Bob,6), (Mike,5).

NEW QUESTION # 15

Refer to the exhibit.

Group By and Display Fields Clear All Load Save

Attribute	Order	Display As	Row	Move
Event Receive Time	DESC ▼		+	-
Reporting IP			+	-
Event Type			+	-
Raw Event Log			+	-
COUNT(Matched Events)			+	-

As shown in the exhibit, why are some of the fields highlighted in red?

- A. The Event Receive Time attribute is not available for logs.
- **B. Unique values cannot be grouped.**
- C. No RAW Event Log attribute information is available.
- D. The attribute COUNT(Matched Events) is an invalid expression.

Answer: B

Explanation:

The fields are highlighted in red because unique values such as Event Receive Time and Raw Event Log cannot be used in group-by operations. Grouping requires aggregatable or consistent values across events, while these fields are unique to each event, making them incompatible for grouping.

NEW QUESTION # 16

.....

Free FCP_FSM_AN-7.2 Pdf Guide: https://www.itexamsimulator.com/FCP_FSM_AN-7.2-brain-dumps.html

- Reliable FCP_FSM_AN-7.2 ExamDumps ☐ Reliable FCP_FSM_AN-7.2 Test Review ☐ FCP_FSM_AN-7.2 Reliable Braindumps Files ☐ Search for ✓ FCP_FSM_AN-7.2 ☐ ✓ ☐ on ➡ www.prepawayete.com ☐ immediately to obtain a free download ☐ New FCP_FSM_AN-7.2 Exam Guide
- Trustworthy FCP_FSM_AN-7.2 Valid Mock Test Offers Candidates Pass-Sure Actual Fortinet FCP - FortiSIEM 7.2 Analyst Exam Products ☐ Download ☐ FCP_FSM_AN-7.2 ☐ for free by simply entering ⇒ www.pdfvce.com ⇐ website ☐ Reliable FCP_FSM_AN-7.2 Test Review
- Prepare with updated Fortinet FCP_FSM_AN-7.2 dumps - Get up to 1 year of free updates ☐ Simply search for ► FCP_FSM_AN-7.2 ◀ for free download on 「 www.examdisscuss.com 」 ☐ Reliable FCP_FSM_AN-7.2 Test Review
- FCP_FSM_AN-7.2 Valid Test Experience ☐ FCP_FSM_AN-7.2 Study Dumps ☐ FCP_FSM_AN-7.2 New Braindumps Ebook ☐ Search for { FCP_FSM_AN-7.2 } and obtain a free download on 「 www.pdfvce.com 」 ☐ ☐ Testking FCP_FSM_AN-7.2 Exam Questions
- 2026 FCP_FSM_AN-7.2 – 100% Free Valid Mock Test | Accurate Free FCP_FSM_AN-7.2 PdfGuide ☐ (www.testkingpass.com) is best website to obtain ► FCP_FSM_AN-7.2 ☐ for free download ☐ New FCP_FSM_AN-7.2 Exam Guide
- Valid FCP_FSM_AN-7.2 Valid Mock Test Offer You The Best Free PdfGuide | FCP - FortiSIEM 7.2 Analyst ☐ Easily obtain ☐ FCP_FSM_AN-7.2 ☐ for free download through ☐ www.pdfvce.com ☐ ☐ FCP_FSM_AN-7.2 New Braindumps Ebook
- Reliable FCP_FSM_AN-7.2 ExamDumps ☐ Testking FCP_FSM_AN-7.2 Exam Questions ☐ Pdf FCP_FSM_AN-7.2 Exam Dump ☐ Search on (www.examcollectionpass.com) for { FCP_FSM_AN-7.2 } to obtain exam materials for free download ☐ FCP_FSM_AN-7.2 Download Fee
- Free PDF 2026 Fortinet High-quality FCP_FSM_AN-7.2: FCP - FortiSIEM 7.2 Analyst Valid Mock Test ☐ The page for free download of ☐ FCP_FSM_AN-7.2 ☐ on [www.pdfvce.com] will open immediately ☐ FCP_FSM_AN-7.2 New Braindumps Ebook
- 2026 FCP_FSM_AN-7.2 – 100% Free Valid Mock Test | Accurate Free FCP_FSM_AN-7.2 PdfGuide ☐ The page for free download of ✓ FCP_FSM_AN-7.2 ☐ ✓ ☐ on “ www.prepawaypdf.com ” will open immediately ☐

□FCP_FSM_AN-7.2 Study Dumps

- Latest FCP_FSM_AN-7.2 Learning Materials □ Valid Dumps FCP_FSM_AN-7.2 Ebook □ Valid Dumps FCP_FSM_AN-7.2 Book □ Open ⇒ www.pdfvce.com ⇐ enter 「 FCP_FSM_AN-7.2 」 and obtain a free download □Reliable FCP_FSM_AN-7.2 Test Review
- FCP_FSM_AN-7.2 practice questions - FCP_FSM_AN-7.2 latest torrent - FCP_FSM_AN-7.2 training material □ Enter ➡ www.examdiscuss.com □ and search for 「 FCP_FSM_AN-7.2 」 to download for free □Valid Dumps FCP_FSM_AN-7.2 Ebook
- swipy.ru, onlyfans.com, fortunetelleroracle.com, telegra.ph, kaeuchi.jp, swipy.ru, www.fundable.com, fortunetelleroracle.com, scalar.usc.edu, learn.csisafety.com.au, Disposable vapes

P.S. Free & New FCP_FSM_AN-7.2 dumps are available on Google Drive shared by ITExamSimulator:
https://drive.google.com/open?id=1C8W_tx45eLav0jkytU6_KCHTsaPgfkP4