

# FCP\_FSM\_AN-7.2的中率、FCP\_FSM\_AN-7.2参考書勉強



P.S. Fast2testがGoogle Driveで共有している無料かつ新しいFCP\_FSM\_AN-7.2ダンプ： <https://drive.google.com/open?id=1nrNcSq7KpNt2u3iDqMaxQBwOgWLKMKDc>

FCP\_FSM\_AN-7.2テスト資料は、ユーザーが勉強するたびに合理的な配置であり、可能な限りユーザーが最新のFCP\_FSM\_AN-7.2試験トレントを長期間使用しないようにします。ユーザーが知識を習得する必要があるたびにFCP\_FSM\_AN-7.2練習教材は、ユーザーがこの期間に学習タスクを完了することができる限り、FCP\_FSM\_AN-7.2テスト教材は自動的に学習システムを終了し、ユーザーに休憩を取るよう警告します。次の学習期間に備えてください。

## Fortinet FCP\_FSM\_AN-7.2 認定試験の出題範囲：

トピック	出題範囲
トピック 1	<ul style="list-style-type: none"><li>機械学習、UEBA、ZINA: このセクションでは、上級セキュリティアーキテクトのスキルを評価し、最新のセキュリティテクノロジーの統合について学びます。機械学習モデルの設定タスクの実行、UEBA（ユーザーおよびエンティティの行動分析）データをルールやダッシュボードに組み込んで脅威検出を強化すること、そしてZTNA（ゼロトラスト・ネットワーク・アクセス）の原則をセキュリティ運用に統合する方法を理解することが求められます。</li></ul>
トピック 2	<ul style="list-style-type: none"><li>インシデント、通知、および修復: このセクションでは、インシデント対応者のスキルを評価し、インシデント管理ライフサイクル全体を網羅します。これには、セキュリティインシデントの管理と優先順位付け、アラート通知のポリシー設定、脅威の封じ込めと解決のための自動修復アクションの設定に必要なスキルが含まれます。</li></ul>
トピック 3	<ul style="list-style-type: none"><li>ルールとサブパターン: このセクションでは、SOCエンジニアのスキルを評価し、分析ルールの構築と実装に焦点を当てます。ルールを構成する様々なコンポーネントの特定、サブパターンや集約といった高度な機能の活用、そしてFortiSIEMプラットフォーム内でこれらのルールを実際に設定してセキュリティイベントを検知するスキルが問われます。</li></ul>

トピック 4	<ul style="list-style-type: none"> <li>分析: このセクションでは、セキュリティアナリストのスキルを評価し、クエリの構築と改良に関する基礎的な手法を網羅します。イベントからの検索の作成、グループ化と集計手法の適用、CMDBやネストされたクエリを含む様々なルックアップ操作の実行など、データの効果的な分析と相関分析に重点が置かれます。</li> </ul>
--------	--

>> FCP\_FSM\_AN-7.2的中率 <<

## FCP\_FSM\_AN-7.2参考書勉強、FCP\_FSM\_AN-7.2日本語pdf問題

Fast2testのFCP\_FSM\_AN-7.2トレーニングテストの利点の1つは、無料の販売前体験をユーザーに提供できることです。FCP\_FSM\_AN-7.2学習資料ページはサンプルの質問モジュールを提供します。Fortinet購入する前に、ユーザーはさらにFCP\_FSM\_AN-7.2のFCP - FortiSIEM 7.2 Analyst試験準備を使用します。同時に、提供するサンプルユーザーがPDFデモを無料でダウンロードできる方が便利のため、販売前の体験は他に類を見ません。そのため、FCP\_FSM\_AN-7.2学習教材の効率性を把握し、間違いなく選択することを決定できます。

## Fortinet FCP - FortiSIEM 7.2 Analyst 認定 FCP\_FSM\_AN-7.2 試験問題 (Q49-Q54):

### 質問 # 49

Refer to the exhibit.

Source IP	Reporting Device	Reporting IP	Event Type	User	Application Category
15.2.3.4	FW01	10.1.1.1	Logon	Mike	DB
21.3.4.5	FW02	10.1.1.2	Logon	Bob	WebApp
14.12.3.1	FW01	10.1.1.1	Logon	Alice	SSH
192.168.1.5	FW03	10.1.1.3	Logon	Alice	DB
10.1.1.1	FW01	10.1.1.1	Logon	Bob	DB
123.123.1.1	FW04	10.1.1.4	Logon	Mike	SSH

If you group the events by Reporting Device, Reporting IP, and Application Category, how many results will FortiSIEM display?

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

正解: E

解説:

Grouping by Reporting Device, Reporting IP, and Application Category yields five unique tuples: (FW01, 10.1.1.1, DB), (FW02, 10.1.1.2, WebApp), (FW01, 10.1.1.1, SSH), (FW03, 10.1.1.3, DB), and (FW04, 10.1.1.4, SSH).

### 質問 # 50

From which two sources can you import data to train FortiSIEM machine learning? (Choose two.)

- A. FortiSIEM reports
- B. Syslog archives
- C. SQL database
- D. CSV files

正解: A、D

### 質問 # 51

What are the four incident status values on FortiSIEM?

- A. Active, closed, cleared, resolved
- B. Active, auto closed, cleared manually, resolved
- C. Active, auto cleared, cleared manually, system cleared
- D. Active, cleared, cleared manually, false positive

正解: C

解説:

FortiSIEM incidents can have four status values: Active, Auto Cleared, Cleared Manually, and System Cleared. These statuses track the lifecycle of an incident—from detection (Active) to resolution - whether it's cleared automatically by correlation logic or manually by an analyst.

### 質問 # 52

Refer to the exhibit.

The screenshot shows the 'Automation Policy' configuration page in FortiSIEM. The 'Name' field is 'Automation'. Under 'Severity', 'Low', 'Medium', and 'High' are all checked. The 'Rules' dropdown is set to 'GROUP:Security'. 'Time Range' is 'ANY', 'Affected Items' is 'ANY', and 'Affected Orgs' is 'Rule:Banking'. In the 'Action' section, the following actions are checked: 'Send Email/SMS/Webhook to the target users.', 'Run Remediation/Script.', 'Invoke an Integration Policy. Run: no policy.', and 'Create Case when an incident is created.'. The other actions are unchecked.

According to the automation policy configuration shown in the exhibit, what happens if an associated rule triggers?

- A. FortiSIEM runs the remediation script, because that takes precedence over all other options.
- B. FortiSIEM fails to the integration policy, because no policy is defined.
- C. FortiSIEM performs all selected actions.
- D. FortiSIEM sends an email, because that is first on the list.

正解: C

解説:

When an associated rule triggers, FortiSIEM performs all selected actions in the automation policy. In this case, it will send an email/SMS/webhook, run the remediation script, invoke the integration policy (even if none is currently defined), and create a case. All checked actions are executed.

### 質問 # 53

Refer to the exhibit.

#### Rule Subpattern

The screenshot shows the 'Edit SubPattern' interface for a rule named 'DomainAcctLockout'. It is divided into three main sections: Filters, Aggregate, and Group By. The Filters section contains one filter: 'Event Type' with the operator 'IN' and the value 'EventTypes: Domain Account Lox'. The Aggregate section is configured with 'COUNT(Matched Events)' and the operator '>=' followed by the value '1'. The Group By section is set to 'Attribute' and lists 'Reporting Device', 'Reporting IP', and 'User'. At the bottom, there are buttons for 'Run as Query', 'Save as Report', 'Save', and 'Cancel'.

Which section contains the subpattern configuration that determines how many matching events are needed to trigger the rule?

- A. Group By
- B. Actions
- C. Filters
- D. Aggregate

正解: D

解説:

The Aggregate section contains the condition COUNT(Matched Events) >= 1, which defines how many events must match the filter criteria for the rule to trigger. This is the subpattern configuration that determines the event threshold.

### 質問 # 54

.....

君は一回だけでFortinetのFCP\_FSM\_AN-7.2認定試験に合格したいなら、或いは自分のIT技能を増強したいなら、Fast2testはあなたにとって最高の選択です。長年の努力を通じて、Fast2testのFortinetのFCP\_FSM\_AN-7.2認定試験の合格率が100パーセントになっていました。うちのFortinetのFCP\_FSM\_AN-7.2試験問題集は完全な無制限のダンプが含まれているから、使ったら気楽に試験に合格することができます。

FCP\_FSM\_AN-7.2参考書勉強: [https://jp.fast2test.com/FCP\\_FSM\\_AN-7.2-premium-file.html](https://jp.fast2test.com/FCP_FSM_AN-7.2-premium-file.html)

- FCP\_FSM\_AN-7.2試験解答 □ FCP\_FSM\_AN-7.2資格勉強 □ FCP\_FSM\_AN-7.2資格難易度 □ □  
jp.fast2test.com □ から簡単に { FCP\_FSM\_AN-7.2 } を無料でダウンロードできますFCP\_FSM\_AN-7.2日本語解説集
- FCP\_FSM\_AN-7.2関連日本語版問題集 □ FCP\_FSM\_AN-7.2試験情報 □ FCP\_FSM\_AN-7.2試験情報 □  
今すぐ ▶ [www.goshiken.com](http://www.goshiken.com) □ を開き、☀ FCP\_FSM\_AN-7.2 □ ☀ □ を検索して無料でダウンロードしてくださいFCP\_FSM\_AN-7.2関連日本語版問題集
- FCP\_FSM\_AN-7.2試験 □ FCP\_FSM\_AN-7.2関連問題資料 □ FCP\_FSM\_AN-7.2対応受験 □ 今すぐ ✓  
[www.passtest.jp](http://www.passtest.jp) □ ✓ □ で [ FCP\_FSM\_AN-7.2 ] を検索し、無料でダウンロードしてくださいFCP\_FSM\_AN-7.2資格難易度
- FCP\_FSM\_AN-7.2試験問題集、FCP\_FSM\_AN-7.2試験テストエンジン、FCP\_FSM\_AN-7.2試験学習ガイド  
□ 《 [www.goshiken.com](http://www.goshiken.com) 》にて限定無料の □ FCP\_FSM\_AN-7.2 □ 問題集をダウンロードせよ  
FCP\_FSM\_AN-7.2問題と解答
- 権威のあるFCP\_FSM\_AN-7.2の中率 - 合格スムーズFCP\_FSM\_AN-7.2参考書勉強 | 有難いFCP\_FSM\_AN-7.2日本語pdf問題 □ ▶ [www.goshiken.com](http://www.goshiken.com) ◀ サイトで □ FCP\_FSM\_AN-7.2 □ の最新問題が使えるFCP\_FSM\_AN-7.2テスト対策書

- 高品質FCP\_FSM\_AN-7.2的中率 - 資格試験におけるリーダーオファー - 有効的なFCP\_FSM\_AN-7.2:FCP - FortiSIEM 7.2 Analyst □ ( www.goshiken.com ) で使える無料オンライン版□FCP\_FSM\_AN-7.2 □の試験問題FCP\_FSM\_AN-7.2対応受験
- 試験FCP\_FSM\_AN-7.2的中率 - 一生懸命にFCP\_FSM\_AN-7.2参考書勉強 | ユニークなFCP\_FSM\_AN-7.2日本語pdf問題 □ [ www.passtest.jp ]の無料ダウンロード⇒FCP\_FSM\_AN-7.2 □ページが開きますFCP\_FSM\_AN-7.2試験関連情報
- 100%合格率のFCP\_FSM\_AN-7.2的中率 - 合格スムーズFCP\_FSM\_AN-7.2参考書勉強 | 効率的なFCP\_FSM\_AN-7.2日本語pdf問題 □ ⇒ www.goshiken.com □で使える無料オンライン版⇒FCP\_FSM\_AN-7.2 □□□の試験問題FCP\_FSM\_AN-7.2過去問
- FCP\_FSM\_AN-7.2必殺問題集 □FCP\_FSM\_AN-7.2模擬対策問題 □FCP\_FSM\_AN-7.2模擬対策問題 □ウェブサイト▶ www.xhs1991.com ◀から「FCP\_FSM\_AN-7.2」を開いて検索し、無料でダウンロードしてくださいFCP\_FSM\_AN-7.2資格難易度
- FCP\_FSM\_AN-7.2過去問題 □FCP\_FSM\_AN-7.2必殺問題集 □FCP\_FSM\_AN-7.2認定内容 □ ✓ www.goshiken.com □✓□に移動し、 ⇒ FCP\_FSM\_AN-7.2 □を検索して無料でダウンロードしてくださいFCP\_FSM\_AN-7.2認定内容
- 100%合格率のFCP\_FSM\_AN-7.2的中率 - 合格スムーズFCP\_FSM\_AN-7.2参考書勉強 | 効率的なFCP\_FSM\_AN-7.2日本語pdf問題 □ ⇒ www.passtest.jp □に移動し、【FCP\_FSM\_AN-7.2】を検索して、無料でダウンロード可能な試験資料を探しますFCP\_FSM\_AN-7.2資格難易度
- mysocialquiz.com, deweyshio784139.tnpwiki.com, brendagrivr815337.smblogsites.com, larafeqe554067.evawiki.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bookmarkextent.com, bookmarkfavours.com, songtr.ee, thesocialdelight.com, bytecomputer.in, Disposable vapes

無料でクラウドストレージから最新のFast2test FCP\_FSM\_AN-7.2 PDFダンプをダウンロードする：<https://drive.google.com/open?id=1nrNcSq7KpNt2u3iDqMaxQBwOgWLKMKDc>