CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFA認定試験ガイド

説明

CrowdStrike Certified Falcon Administrator（CCFA）認定試験は、CCFA認定の修了に向けた最終ステップです。この試験では、センサーのインストールを含め、CrowdStrike Falcon®プラットフォームのさまざまなコンポーネントを毎日管理するための受験者の知識、スキル、能力を評価します。

CrowdStrike Certified Falcon Administratorとして合格すると、次のことができます。

- ユーザー管理とロールベースの権限について理解する
- Falconセンサーを展開および管理し、グループを作成する
- 展開および防止ポリシー設定を構成する
- 許可リストとブロックリストを設定する
- 除外を設定する
- 管理レポートを実施する

CrowdStrike認定プログラム

要件

すべての試験登録者は、次の条件を満たす必要があります（例外はありません）。

- **CrowdStrike認定試験同意書に同意する**
- 18歳以上である
- CrowdStrike試験バウチャーを購入する

見積もりの依頼や、Pearson VUEを通じたCrowdStrike試験バウチャーの購入については、クラウドストライクのアカウントエグゼクティブにお問い合わせください。

Universityサブスクリプション

すべての試験登録者がCrowdStrike Universityのアクティブなサブスクリプションを保有し、CrowdStrike Universityアカウントへのアクセスを確認することを**強くお勧めします**。

- CrowdStrike認定に準拠したコースは、アクティブなCrowdStrike Universityアカウントを持つ学習者が利用できます。
- 一意のCrowdStrike認定ID、トレーニング成績証明書、印刷可能な認定文書は、CrowdStrike University学習管理システムを通じて入手できます。

注：すべての受験者は、Pearson VUEを通じてCrowdStrike認定試験スコアレポートを表示および印刷できます。

認定志願者に求められる適性と能力

- 志願者は、本番環境において6か月以上のCrowdStrike Falconの使用経験がある必要があります。

2023 CrowdStrike, Inc.All rights reserved.

試験について

評価方法

CCFA認定試験は、90分間で60問に解答する必要があります。試験問題は、トリッキーな言葉遣い、二重否定、および穴埋め式の問題を排除して明確に書かれています。この試験は、技術者と非技術者の両者による複数回の編集を経たうえで、さまざまな志願者によってテストされています。

初期認定

認定を受けるうえで、志願者は次の条件を満たしている必要があります。

- CCFA認定試験で合格点を獲得する
- いかなる不正行為も行わない

志願者による不正行為があった場合、クラウドストライクは、スコアを無効にし、疑わしい行為を**CrowdStrike認定試験同意書**に対する違反とみなすことができます。

志願者が試験を完了し、志願者の公式試験スコアが投稿された後、認定志願者は、Pearson VUEで公式試験スコアを確認できます。

再受験ポリシー

受験1回目で試験に合格しなかった志願者には、次のことが求められます。

- 試験を再受験するにあたり、48時間待機する必要があります（待機時間は試験後から始まります）。
- このドキュメントに記載されている試験の目的、トレーニングコースの資料、および関連する推奨資料を確認する必要があります。

2回目の受験後、志願者は、3回目およびそれ以降の受験にあたり、7日間待機する必要があります。待機時間は、受験の翌日から始まります。

再受験を希望する志願者は、再挑戦する前に、該当する推奨されるコースを再受講し、CrowdStrike Falconでの追加の経験を積むことを検討する必要があります。

4回目以降の再受験は、ケースバイケースで検討されます。クラウドストライクは、4回目以降の再受験を拒否する権利を有します。

以前に合格した試験の再受験

志願者は、クラウドストライクによって承認された再認定要件に直接関連しない限り、以前に合格した試験を再受験することはできません。

ベータ試験

志願者は、ベータ試験を再受験することはできません。

試験に対する異議申し立て

試験に誤りがある、またはCCFA試験の特定の設問が無効であると認定志願者が確信する場合は、certification@crowdstrike.comに連絡して、請求の評価を申請してください。請求が検討されるためには、認定志願者は試験を受けてから3日以内に請求を提出する必要があります。クラウドストライクは、通常、15営業日以内に提起された内容に関して対応します。

再認定

認定試験は製品バージョンに関連付けられていません。今後の再認定については、認定が発行された日付を起点として、次のライフサイクルが適用されます。

- CrowdStrike Certified Falcon Administrator（CCFA）：3年
- CrowdStrike Certified Falcon Responder（CCFR）：3年
- CrowdStrike Certified Falcon Hunter（CCFH）：3年

2023 CrowdStrike, Inc.All rights reserved.

試験の準備

推奨トレーニング

クラウドストライクでは、認定志願者がCCFA認定試験の準備をするために、CrowdStrike Universityのこれらの**CSU LP-A: Falcon Administrator**コースを修了することを強くお勧めします。これらのコースの詳細については、**CrowdStrikeトレーニングカタログ**をご覧ください。

推奨資料

クラウドストライクでは、認定志願者がCCFA認定試験の準備をするために、次のタイトルのCrowdStrike Falconサポートドキュメントを復習することを強くお勧めします。

- センサーのデプロイメントおよびメンテナンス
- Falcon Management
- エンドポイントセキュリティ - 「レスポンス」、「設定」、「追加機能」の各セクション
- CrowdStrikeストア
- CrowdStrike API - 全般情報

出題範囲

次のトピックは、試験に含まれる可能性のある内容の一般的なガイドラインを提供します。ただし、他の関連トピックが試験の特定の実施に含まれる場合もあります。

1. ユーザー管理
2. センサーの展開
3. ホストの管理
4. グループの作成
5. 防止ポリシー
6. カスタムIOAルール
7. センサー更新ポリシー
8. ファイルの隔離
9. IOC管理
10. 隔離ポリシー
11. 除外
12. レポート
13. リアルタイムレスポンスポリシー／監査ログ
14. APIクライアントおよびキー
15. 通知ワークフロー

範囲の変更

以下のガイドラインは、試験の内容をよりよく反映し、わかりやすくするために、いつでも予告なしに変更される場合があります。このような変更には、利用可能なCrowdStrike認定の追加または削除、認定要件の変更、および推奨されるトレーニングコース、試験の目的、概要、および試験（試験のスコアの発行の方法とタイミングが含まれますがこれに限定されません）の変更が含まれますが、これに限定されません。認定志願者は、認定を取得および維持するための条件として、修正されたプログラム要件を満たす（および満たし続ける）ことに同意します。

2023 CrowdStrike, Inc.All rights reserved.

試験の目的

次のサブトピックと学習目標は、試験の内容と目的に関する詳細なガイダンスを提供します。

1.0 ユーザー管理

- **1.1** Falconコンソールの機能にアクセスするために必要なロールを特定する
  - 1.1.1 Falconの各リアルタイムレスポンス（RTR）ロールの機能と制限について説明する
  - 1.1.2 新しいユーザーの作成、ユーザーの削除、ユーザーの編集などを行う

2.0 センサーの展開

- **2.1** Falconセンサーをインストールする前に、インストール前のOS／ネットワークの要件を分析する
- **2.2** デフォルトポリシーを分析し、ベストプラクティスを適用してFalconセンサーのワークロードを準備する
- **2.3** 適切な設定を適用して、Windows、Linux、およびmacOSにFalconセンサーを正常にインストールする
  - 2.3.2 イメージ／VDI、トークン、およびタグの追加／詳細オプションを適用する
- **2.4** センサーをアンインストールする
- **2.5** トラブルシューティング
  - 2.5.1 システム環境またはFalconコンポーネントの基本的な設定要件に関する問題を認識する
  - 2.5.2 ポリシーの設定、権限、しきい値に関する問題を解決する
  - 2.5.3 Falcon診断ログを収集し、センサーの問題を分析する

3.0 ホストの管理

- **3.1** 「Host Management（ホストの管理）」ページでフィルターを使用する方法を提案する
- **3.2** ホストに対して検知を無効化する
- **3.3** ホストでの検知を無効化した場合の影響について説明する
- **3.4** 機能制限モード（RFM）の影響とその原因 について説明する
- **3.5** RFMのホストを見つける
- **3.6** 非アクティブなセンサーを見つける
- **3.7** 非アクティブなセンサーの保持期間を確認し、データバックアップ計画を定義する
- **3.8** ホストに関する情報をレポートするときに使用するレポートを特定する

4.0 グループの作成

- **4.1** エンドポイントの適切なグループ割り当てを特定し、これがポリシーの適用にどのように影響するかを理解する
  - 4.1.1 ポリシーのタイプ、コンポーネント、適用、およびワークフローについて説明する
  - 4.1.2 優先順位、グループ、およびベストプラクティスを定義する

2023 CrowdStrike, Inc.All rights reserved.

5.0 防止ポリシー

- **5.1** エンドポイントの適切な防止ポリシー設定を特定し、これがセキュリティポスチャにどのように影響するかについて説明する
  - 5.1.1 デフォルトのポリシーの使用目的を実証し、デフォルトポリシーを設定する際のベストプラクティスを適用する
  - 5.1.2 検知のみのポリシーを設定する
  - 5.1.3 「センサー上」にある機械学習と「クラウド」にある機械学習について説明する
  - 5.1.4 さまざまなポリシー設定オプションのそれぞれの機能について説明する
  - 5.1.5 次世代AV設定を定義する
  - 5.1.6 エンドユーザー通知の機能について説明する
  - 5.1.7 グループとホストに防止ポリシーを割り当てる
  - 5.1.8 防止ポリシーに関する優先順位について説明する
  - 5.1.9 ポリシーのベストプラクティスについて説明する

6.0 カスタムIOAルール

- **6.1** 根本的に悪意のない振る舞いをモニタリングするためのカスタムIOA（攻撃の痕跡）ルールを作成する

7.0 センサー更新ポリシー

- **7.1** 更新プロセスを制御するための適切なセンサー更新ポリシー設定と関連する全般設定を特定する
  - 7.1.1 更新ポリシーを定義する
  - 7.1.2 デフォルトのポリシーの使用目的を実証し、デフォルトポリシーを設定する際のベストプラクティスを適用する
  - 7.1.3 自動更新の機能について説明する
  - 7.1.4 MAC／Win／*nixの個別のポリシーについて説明する
  - 7.1.5 単一のセンサーまたは環境全体でビルドバージョンが表示される場所について説明する
  - 7.1.6 センサー更新ポリシーに関する優先順位について説明する

8.0 隔離ファイル

- **8.1** 隔離ファイルを管理するために必要なオプションを適用する

9.0 IOC管理

- **9.1** セキュリティポスチャのカスタマイズとフォルスポジティブの管理に必要なIOC設定を評価する

2023 CrowdStrike, Inc.All rights reserved.

10.0 隔離ポリシー

- **10.1** セキュリティワークフローの要件に基づいて、ネットワークが隔離されているときに適切なIPアドレスの許可リストを設定する
- **10.2** 隔離ポリシーの機能について説明する

11.0 除外

- **11.1** ビジネス要件を解釈して、信頼できるアクティビティを許可し、フォルスポジティブを解決し、パフォーマンスの問題を修正する
  - 11.1.1 glob構文を使用して有効なファイル除外ルールを作成する
  - 11.1.2 グループにファイルパターン除外を適用する
  - 11.1.3 除外ルールの管理方法を実証する

12.0 センサーレポート

- **12.1** さまざまなタイプのセンサーレポートと各レポートで提供される情報について説明する
  - 12.1.1 機械学習防止モニタリングレポートに含まれる情報について説明する
  - 12.1.2 Falcon UI監査証跡レポートに含まれる情報について説明する
  - 12.1.3 API監査証跡、防止ポリシー監査証跡、および無視された防止ハッシュレポートに含まれる情報について説明する
  - 12.1.4 防止ポリシーデバッグレポートに含まれる情報について説明する

13.0 リアルタイムレスポンスポリシー／監査ログ

- **13.1** ロールおよびポリシー設定を適用し、RTR監査ログを追跡および確認して、ユーザーアクティビティを管理する

14.0 APIクライアントおよびキー

- **14.1** APIキーを管理する

15.0 通知ワークフロー

- **15.1** ポリシー、検知、インシデントについて個人に通知するためのカスタムアラートを設定する

2023 CrowdStrike, Inc. All rights reserved.