CrowdStrike University

CROWDSTRIKE

CROWDSTRIKE UNIVERSITY

CCFR認定試験ガイド

説明

CrowdStrike Certified Falcon Responder（CCFR）認定試験は、CCFR認定の修了に向けた最終ステップです。この試験では、CrowdStrike Falcon®コンソール内の検知に対応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 Responderとして合格すると、次のことができます。

- Falconコンソールで検知の初期トリアージを行う
- 検知のフィルタリング、グループ化、割り当て、コメントの追加、およびステータスの変更を管理する
- ホスト検索、ホストタイムライン、プロセスタイムライン、ユーザー検索、その他のクリック駆動型ワークフローなどの基本的な調査タスクを実行する
- エンタープライズイベントデータ全体にわたり、ドメイン名、IPアドレス、ハッシュ値などのアトミックインジケーターの基本的なプロアクティブハンティングを実施する

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認定試験同意書を受け入れる**
- 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。

ユニバーシティ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。

試験について

評価方法

CCFR認定試験は、90分間に60問の設問に解答する評価です。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。

- CCFR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プラットフォーム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留保します。技術的な問題が原因で4回目の試験に失敗した場合、受講生は5回目に挑戦できます。

個人的なパフォーマンスが原因で4回目の試験に失敗した場合、受講生は、30日間待機したうえで、試験ガイドに示されている推奨トレーニングを再受講する必要があります。クラウドストライクは、志願者が試験ガイドで推奨されているトレーニングを再受講したこと、およびCS認定マネージャーと面談したことを確認してから、5回目の試験への登録を許可します。

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CCFR認定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

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CCFR認定試験の準備をするために、CrowdStrike Universityのこれらの**CSU LP- R: Incident Responder**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CCFR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。

- Falcon管理 -『Falcon Console User Guide（Falconコンソールユーザーガイド）』、「Dashboards and Reports（ダッシュボードとレポート）」セクション
- エンドポイントセキュリティ -「Start Up and Scale Up（スタートアップとスケールアップ）」、「Monitoring（モニタリング）」、「Event Investigation（イベント調査）」、および「Response（レスポンス）」セクション

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。

- 1.0　攻撃のフレームワーク
- 2.0　検知の解析
- 3.0　イベントの検索
- 4.0　ハンティング解析
- 5.0　ハンティング方法

- 6.0 ナビゲーション
- 7.0 レポート
- 8.0 検索ツール

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。

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 攻撃のフレームワーク

- 1.1 Falcon内でMITRE ATT&CK情報を使用して、コンテキストを検知に提供する
- 1.2 MITRE ATT&CKフレームワークで提供される情報について説明する

2.0 検知の解析

- 2.1 Falconプラットフォーム内で提供された情報の解析に基づいて行動方針を推奨する
- 2.2 検知ダッシュボードに表示される一般的な情報について説明する
- 2.3 「Activity（アクティビティ）」>「Detections（検知）」ページに表示される情報について説明する
- 2.4 Falconプラットフォーム内のさまざまな検知ソースについて説明する
- 2.5 ホスト検索の結果に含まれるデータを解釈する
- 2.6 ハッシュ検索の結果に含まれるデータを解釈する
- 2.7 検知からプロセスタイムラインに移動する方法を実証する
- 2.8 検知で利用できるコンテキストイベントデータ（IP、DNS、ディスクなど）について説明する
- 2.9 検知フィルタリングとグループの使用方法について説明する
- 2.10 組み込みのOSINTツールを使用するタイミングについて説明する

- 2.11 グローバル普及率とローカル普及率の違いについて説明する
- 2.12 「Full Detection Details（検知結果の詳細）」で提供される内容について説明する
- 2.13 「Full Detection Details（検知結果の詳細）」にアクセスする方法について説明する
- 2.14 「Full Detection Details（検知結果の詳細）」に含まれる情報を使用してプロセスの関係を解析する
- 2.15 「View As Process Tree（プロセスツリーで表示）」、「View As Process Table（プロセステーブルで表示）」、および「View As Process Activity（プロセスアクティビティで表示）」で提供されるデータのタイプについて説明する
- 2.16 ホスト検索中にエンドポイントの管理対象／管理対象外の近隣アセットを識別する方法について説明する
- 2.17 検知をアナリストに割り当てる目的について説明する
- 2.18 Falcon UIで非Falconの侵害の痕跡（IOC）をトリアージする
- 2.19 さまざまなポリシー（「Block（ブロック）」、「Block and Hide Detection（検知をブロックして非表示にする）」、「Detect Only（検知のみ）」、「Allow（許可）」、「No Action（アクションなし）」）の機能について説明する
- 2.20 許可リストとブロックリストに登録した場合の影響について説明する
- 2.21 機械学習から除外ルールの影響について説明する
- 2.22 「Sensor Visibility exclusions（センサー可視性から除外）」の影響について説明する
- 2.23 「IOA exclusions（IOA除外）」の影響について説明する
- 2.24 隔離されたファイルの保存期間について説明する
- 2.25 隔離されたファイルをリリースした場合の結果について説明する
- 2.26 隔離されたファイルをダウンロードする
- 2.27 検知に基づき、使用する調査ツール（ホスト、ハッシュなど）をベストプラクティスに基づいて決定する

3.0 イベントの検索

- 3.1 検知からイベント検索を実行し、イベントアクションを使用して検索を絞り込む
- 3.2 イベントアクションの機能について説明する
- 3.3 主要なイベントタイプについて説明する

4.0 ハンティング解析

- 4.1 プロセスのタイムラインで提供される情報について説明する
- 4.2 ホストのタイムラインで提供される情報について説明する

5.0 ハンティング方法

- 5.1 プロセスの関係（ターゲット／親／コンテキスト）について説明する

6.0 ナビゲーション

- 6.1 プロセスタイムラインの生成に必要な情報を取得する
- 6.2 イベント検索からプロセスエクスプローラーにアクセスする方法を実演する
- 6.3 隔離されたファイルを検索する

7.0 レポート

- 7.1 詳細なレビューのために「Full Detection Details（検知結果の詳細）」から検知およびプロセスデータをエクスポートする
- 7.2 検知アクティビティレポートに表示される情報について説明する
- 7.3 エグゼクティブサマリーダッシュボードに表示される情報について説明する
- 7.4 検知解決ダッシュボードに表示される情報について説明する

8.0 検索ツール

- 8.1 ユーザー検索で提供される情報について説明する
- 8.2 IP検索で提供される情報について説明する
- 8.3 ハッシュの実行（検索）で提供される情報について説明する
- 8.4 ハッシュ検索で提供される情報について説明する
- 8.5 Bulk domains（一括ドメイン）検索で提供される情報について説明する