CrowdStrike University

CROWDSTRIKE UNIVERSITY

FALCON 200
FALCON PLATFORM FOR ADMINISTRATORS

コース概要

CrowdStrike Falcon®プラットフォームによる侵害の阻止は、堅牢な構成から始まります。組織を効果的に保護できるように、FALCON 200: Falcon Platform for Administratorsでは、ホストを保護するためのベストプラクティスの設定について学習します。

このコースは、Falconプラットフォームを日常的に使用する人を対象としており、プラットフォームのインストール、設定、管理に焦点を当てています。Falcomプラットフォームを管理、使用することになる技術者を想定しています。このコースでは、受講者はセンサーのインストール、防止ポリシー、ユーザー、グループの設定、検知の微調整を行います。

学習内容

- 最新のOS固有のFalconセンサーを環境にインストールし、展開する
- ベストプラクティスに従ってポリシー、ユーザー、ホストグループを設定し、環境を確実に保護する
- Falconダッシュボードとレポートを利用して、組織の環境に適切なカバレッジが含まれること、エンドポイントに最新のセンサーの更新が適用されていることを確認する
- 侵害の痕跡（IOC）の管理と除外で検知を微調整する

前提条件

- コンピューターネットワーキングの概念とプロトコル、ネットワークセキュリティ方法論、プライバシー原則、サイバー脅威と脆弱性の知識
- CSUのFalcon Administrator向けラーニングパス内のeラーニングコースの修了
- Microsoft Windows環境への習熟

要件

- ブロードバンドインターネット接続環境、Webブラウザ、マイクおよびスピーカー
- デュアルモニターおよびヘッドセットの用意を推奨

クラス教材

各種参考資料は、トレーニング当日にCrowdStrike Universityからアクセスできます。

1日プログラム | 2クレジット

このインストラクター主導のコースには、CrowdStrike Falconプラットフォームの説明と、グループとポリシーの作成、センサーのインストールに関するハンズオン演習が含まれています。

次のような場合にこのクラスを受講してください。

- システム管理者またはセキュリティエンジニアである
- CrowdStrike Certified Falcon Administrator（CCFA）試験の準備をしている

登録

スケジュール済みのコースリストと登録情報へのアクセスについては、ご自身のCrowdStrike Universityアカウントにログインしてください。このコースには、2トレーニングクレジットが必要です。CrowdStrike Universityへのアクセス権がない場合は、トレーニングクレジットをご購入いただく必要があります。詳細については、sales@crowdstrike.comまでお問い合わせください。

最終更新：2023年11月28日

CrowdStrike University

FALCON 200 Falcon Platform for Administrators

ユーザーの管理

- 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確認する
- 新しいユーザーの作成、ユーザーの削除、ユーザーの編集を行う

センサーの展開

- 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／ネットワーキング要件を分析する
- 適切な設定を適用して、Windows、Linux、macOSにFalconセンサーを正しくインストールする
- センサーをアンインストールする
- 「Host Management（ホストの管理）」を使用してセンサーのプロパティを確認する
- 各種のセンサーレポートと各レポートの内容について説明する
- 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
- 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確認する

グループ作成

- 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把握する
- 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
- 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

防止ポリシー

- エンドポイントの適切な防止ポリシー設定を特定し、セキュリティポスチャにどのような影響があるかについて説明する

隔離ファイル

- 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

IOC管理

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

除外

- 業務要件を解釈して、信頼できるアクティビティを許可し、フォールスポジティブとパフォーマンスの問題を解決する
- 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
- グループにファイルパターン除外を適用する
- 除外ルールの管理方法を実証する

カスタムIOA、隔離、Falconリアルタイムレスポンス（RTR）

- 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
- 隔離ポリシーの機能について説明する
- セキュリティワークフローの要件に基づいて、ネットワーク隔離時に、適切なIPアドレスを用いて許可リストを設定する
- 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

Falcon Fusionワークフロー

- ポリシー、検知、インシデントについてユーザーに通知するためのワークフローを設定する