CrowdStrike 製品

CROWDSTRIKE

FALCON INTELLIGENCE RECON

オープン、ディープウェブ、およびダークウェブ上の、
ブランド、従業員、および機密データに対する脅威を検知

ダークウェブを超えて、デジタル・リスクを検知

CrowdStrike Falcon Intelligence™ Reconは、オープン、ディープ、ダークウェブから潜在的に悪意のあるアクティビティを検知し、組織が自社のブランド、従業員、機密データをよりよく保護できるようにします。Falcon Intelligence Reconは、何百万もの制限されたウェブページ、犯罪フォーラム、暗号化されたメッセージングプラットフォームからデータを収集し、活動を監視します。セキュリティチームは、リアルタイムでの調査が実行可能となり、組織を標的とする詐欺、データ侵害、フィッシングキャンペーン、およびその他のオンライン脅威を事前に検知できます。

主な機能

収集

Falcon Intelligence Reconは、オープン、ディープウェブ、ダークウェブのアクセスが困難なデジタルチャンネルの8年間以上のデータに瞬時にアクセスできます。Falcon Intelligence Reconは、詐欺行為、盗まれたデータ、企業への脅威、および攻撃者の手法で特定されたエクスプロイトやツールに関する生の情報を積極的に収集します。

- **生の情報を大規模に収集**：何百万ものオープンになっていないウェブページ、何千もの制限されたフォーラム、マーケットプレイス、貼り付けサイト、IRCチャネル、悪質なアプリ、フィッシングドメイン、テレグラム、QQなどのオープンおよびクローズド・メッセージング・アプリケーションからのデータを自動的に監視。
- **リアルタイムに調査を実施**：情報に対しリアルタイムにアクセスし攻撃者グループを崩壊させ、攻撃の機会を制限する。制限されたサイトからのデータに検知不能なアクセスで調査を実施。Falcon Intelligence Reconには履歴データが保存されている為、攻撃者が投稿を変更したり削除しても足跡消去は不可。
- **犯罪に関わる攻撃者グループを追跡**：攻撃者の行動の変化を時間軸で分析、追跡し、活動の増加、新たな攻撃、新たな標的、進化しつつある技術やツールを特定することで、外部からの脅威に対する保護を強化。

主なメリット

- オープン、ディープ、ダークウェブを他に類を見ない方法でカバー
- 何百万もの制限のかかった及びアンダーグラウンドからデータを自動的に抽出
- 調査時間を短縮し、効率と対応を向上
- 組織に合わせたカスタマイズルールによるリアルタイムの監視を提供
- 瞬時のタイム・トゥ・バリュー：導入と運用を数分で完了
- CrowdStrikeの脅威プロファイルとIOCフィード

FALCON INTELLIGENCE RECON

調査

潜在的な脅威をリアルタイムに把握し、組織をターゲットとした不正行為の調査を迅速化します。Falcon Intelligence Reconは、調査報告と分析の厚みを改善するために、より広いコンテキストを提供することによって、リスクの高い推測を避け、従来のインシデント対応を強化します。

- **標的とする脅威の特定**：複雑なクエリを作成することなく、組織に対する外部の脅威であるアンダーグラウンド環境を継続的に監視。Falcon Intelligence Reconは、ブランド名、エグゼクティブ、ドメイン、脆弱性、Eメールアドレスなどの定義済みの検索条件を設定しやすいウィザードを提供。独自の監視ルールを作成、保存し、生の情報をプロアクティブに選別し、チームとの共有が可能。
- **攻撃者を明らかに**：調査結果は、読みやすく表示。ユーザーは、攻撃者とサイトに関する追加のコンテキストを含んだ、オリジナルの脅威アクターの投稿を表示可能。結果はオリジナル言語で表示されるが、ハッカーのスラング辞書を使った拡張翻訳を使い、18の言語から翻訳することが可能。
- **調査の充実**：脅威を完全に把握。ユニバーサル検索では、Falcon Intelligence Reconの結果を、別ライセンス化されているCrowdStrike Falconモジュールが提供する追加コンテキストと自動的に関連付けることが可能。デジタル脅威とエンドポイント検知、ホスト、脅威インテリジェンスレポート、脆弱性などとの関係を明らかにすることで、対応の効率と有効性を最大化を実現。

通知

潜在的な脅威が特定された場合、リアルタイムに通知することで、調査と対応のワークフローを最適化します。トリアージと対応を担当するユーザーが必要な詳細情報を瞬時に入手できるようにします。

- **アラートの優先度を設定**：外部脅威の重要度に基づいてアラートの優先度を設定。通知からアラートの詳細を瞬時に表示します。
- **管理を完全にコントロール**：チームメンバーへの通知方法とアラートの受信頻度をカスタマイズ可能。アラートは迅速に通知されるほか、毎日または毎週などのスケジュールに基づいて通知も可能。基礎となる監視ルールに影響を与えずに、通知のオンとオフを切り替え可能。
- **適切なチームに連絡**：サイバーセキュリティを超えて、デジタルの脅威は組織のブランド、評判、従業員の安全に影響を与えるため、マーケティング、法務、人事、詐欺など、セキュリティ以外の部門に警告も可能。

提供形態

Falcon Intelligence Reconには2つの提供形態があります。

- **Falcon Intelligence Recon Express**：中堅中小企業向け。導入初日からインターネットの隠された領域の偵察を開始します。
- **Falcon Intelligence Recon Enterprise**：Expressの全機能に加えて以下を提供:
  - 進化する調査のための動的なアドホック検索機能
  - クレジットカード/銀行カードのBINデータ
  - CrowdStrike® Intelligence攻撃者グループのプロファイルとIOCフィード

デジタルリスクの再認識

ブランド保護：CrowdStrike Falcon Intelligence Reconは、偽のソーシャルメディアアカウント、ドメイン、モバイルアプリなど、ブランドとの不正なやり取りに関わる攻撃者を発見します。

データ漏洩の発見：CrowdStrike Falcon Intelligence Reconは、オープン、ディープ、ダークウェブに漏洩したデータから、機密データ、IP、クレジットカード情報や認証情報の漏洩を検知します。

サプライ・チェーン監視：CrowdStrike Falcon Intelligence Reconは、チャット、フィッシングキャンペーン、偽造Webサイトなどを公開することで、サプライヤの脅威を特定します。

エグゼクティブ保護：CrowdStrike Falcon Intelligence Reconは、VIPや幹部に対する脅威、なりすまし、フィッシングの試みを監視します。

CROWDSTRIKE について

サイバーセキュリティの世界的リーダーであるCrowdStrikeは、侵害を阻止するために、ゼロから構築したエンドポイント保護プラットフォームを利用し、クラウド時代のセキュリティを再定義しています。CrowdStrike Falcon®プラットフォームの軽量なシングルエージェントアーキテクチャは、クラウドスケール人工知能(AI)を活用し、企業全体にリアルタイムの保護と可視性を提供して、ネットワーク上またはネットワーク外のエンドポイントに対する攻撃を防ぎます。独自のCrowdStrike Threat Graph®を採用したCrowdStrike Falconは、世界で最も高度なセキュリティデータプラットフォームのひとつとして、世界中から取得した週5兆件のエンドポイント関連イベントをリアルタイムで相関分析しています。

次世代AVの無料トライアルの開始

詳細はこちら **www.crowdstrike.jp**