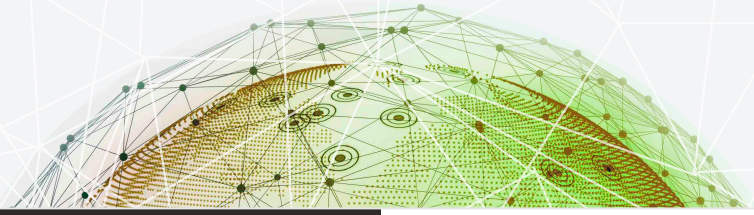
CROWDSTRIKE

FALCON INTELLIGENCE

わかりやすい。的確である。対処方法がわかる。

包括的なサイバー脅威インテリジェンスサービスを利用することで、攻撃者は誰で、どんな手口で、なぜ攻撃してくるのかを把握しましょう。



次にどんな攻撃者がどのような攻撃を仕掛けてくるかを把握している組織は、攻撃が実際に始まる前にその兆候を検知し、次なるサイバー攻撃を阻止することができます。

CrowdStrike Falcon Intelligence™ のグローバルチームは、国家、犯罪者、ハクティビストなど、すべてのタイプの攻撃者を追跡し、破壊的な脅威アクターが組織を攻撃する前に、カスタマイズされた、アクショナブルインテリジェンスを提供します。

業界で認められた実績ある包括的ソリューション

CrowdStrike Falcon Intelligence は、攻撃グループの TTP を徹底的に分析、考察するセキュリティチームを提供して、セキュリティの専門家が現在起きているインシデントを診断して対処できるようにしつつ、将来起こりうるイベントに対してより効果的に対策を立て、高度なマルウェアや標的型の攻撃によるダメージを阻止することができます。

SC Magazine:「充実した詳細情報をうまくまとめた…堅牢なサイバー脅威分析機能」を提供しているとして 5 つ星の評価

SANS Institute: 脅威インテリジェンスのカテゴリーでベストアワードを受賞

主な特長

- **信頼と実績**：CrowdStrike は世界中に潜む 90 以上の攻撃組織のキャンペーンをプロファイルし、分析し、特定することが可能
- **専門性**：自社内そして現場にて人による攻撃者情報の収集、そしてその分析を実施
- **品質**：総合的な分析方法を用いることにより、不要なノイズとなる情報や誤検出を防止
- **柔軟性**：インテリジェンス情報を人が見てわかる形、並びにシステムに取り込むことができるフォーマット両方での提供可能
- **対策につながるアドバイス**：キャンペーンや TTP（タクティクス・テクニック・プロシージャー）を分析することで、それに対する防御策を可能に
- **オーケストレーションとインテグレーション**：API フィードにより、既存のセキュリティインフラへのインテリジェンスの取り込みを自動化

"インテリジェンスとは、あなたから隠れようとする願望を持った攻撃者の情報を収集し、不確実な要素を減らすことである"

– ロバート・M・クラーク（元 CIA 分析官、グループチーフ）

主な特長

インサイトを提供することで組織のセキュリティ体制を強化

- 攻撃者の新たな活動が発生した際に即時アラートで警告
- 一週間ごと、一定期間ごと、四半期ごとの、戦略的な運用・技術レポートの提供
- お客様指定のキーワードや語句に基づいてプロアクティブにアラートを送信
- API、フィードやルールを用いて、SIEM、脅威インテリジェンス・プラットフォームなどの既存インフラへ簡単に統合可能

包括的な分析と脅威インジケーターを組み合わせ、次に予測される脅威を可視化

- 攻撃者の能力、動機、プロファイルの詳細な分析を提供
- 標的型攻撃か、広範囲での攻撃かのいずれかにフォーカスすることで効率的に情報収集が可能
- Falcon Intelligence のインジケーター情報を迅速かつ効率的に検索
- タイムリーなレポートや API フィードを活用して、新たに台頭する脅威への対抗策を迅速に立案可能

"サイバーインテリジェントな防御システムとして、間違いのない逸品。本誌推奨の製品です。"

– SC Magazine

昨今の攻撃の手口は、マルウェアやエクスプロイトだけに限りません。そのため、**Falcon Intelligence** ではコンテキストを意識した、リアルタイムのインテリジェンスで、より多くの脅威を見渡してこれを検知し、その先の侵入を防ぐことができるようセキュリティの専門家を支援します。

Falcon Intelligence には2種類の契約があります。

スタンダード

技術フィードの提供にフォーカスしたインテリジェンスサービス

- ✔ アクターおよびインジケーター API へのアクセス
- ✔ アクタープロファイルを確認できる Web ポータルへのアクセス
- ✔ インジケーター検索
- ✔ Moltego Transforms

プレミアム

包括的なインテリジェンスサービス。プレミアムレベルではスタンダードレベルの内容に加え、以下のサービスが含まれます。

- ✔ レポートとアラート
- ✔ アクター、インジケーター、レポートおよび要件に合ったインテリジェンス API へのアクセス
- ✔ 指定のインテリジェンスカテゴリーで全てのポータルリソースにアクセス可能（Targeted intrusions, eCrime など）
- ✔ フィードとルール
- ✔ テーラーメードのインテリジェンス
- ✔ 必要な情報について調査依頼をアナリストに申請可能
- ✔ マルウェアの分析をアナリストに依頼可能
- ✔ 四半期ごとにインテリジェンスアナリストと1対1のミーティングを実施

CROWDSTRIKE

FALCON INTELLIGENCEの詳細はこちらへお問い合わせください:
japan.sales@crowdstrike.com