CROWDSTRIKE

CROWDSTRIKE FALCON INTELLIGENCE
脅威の自動分析

CROWDSTRIKE FALCON INTELLIGENCE は検知した脅威を自動的に分析します

セキュリティ対策を「プロアクティブ」に変えられる画期的な発明です。

通常の組織では、膨大なセキュリティ・アラートを詳細に分析する時間や専門知識が十分にありません。したがって、新たな脅威に先手を打ってプロアクティブに対応することができておらず、事象が発生するのを待って受動的（リアクティブ）に動いているのが実情です。CrowdStrike® Falcon Intelligence™は、検知した脅威から自動的にその分析を行い、わずか数秒で結果を表示することができる唯一のソリューションであり、「プロアクティブな」防御への転換を可能にします。

エンドポイントに対する攻撃は、クラウド・ネイティブのCrowdStrike Falcon®プラットフォーム基盤で検知されますが、Falcon Intelligenceはそれをそのまま自動的に分析します。サンドボックスでの解析、業界最大のマルウェアデータベースによる関連サンプルの検索、そして脅威インテリジェンスの参照により、Falcon Intelligenceは受けた攻撃に対するトータルな分析結果を数秒で表示します。さらにはカスタマイズされたIOCが生成されますので、それを他のセキュリティツールと共有することができます。この分析によって誰がどのように攻撃してきたかを明らかにし、次にどのようなセキュリティ投資をすべきか、お客様のより正しい意思決定を支援します。

Falcon Intelligenceは、あらゆる規模のお客様に対して、次にどのように対処したら良いのかを明確に示すカスタマイズされた情報を提供するだけでなく、将来の攻撃から組織をどう守るべきかについても明らかにします。

利点

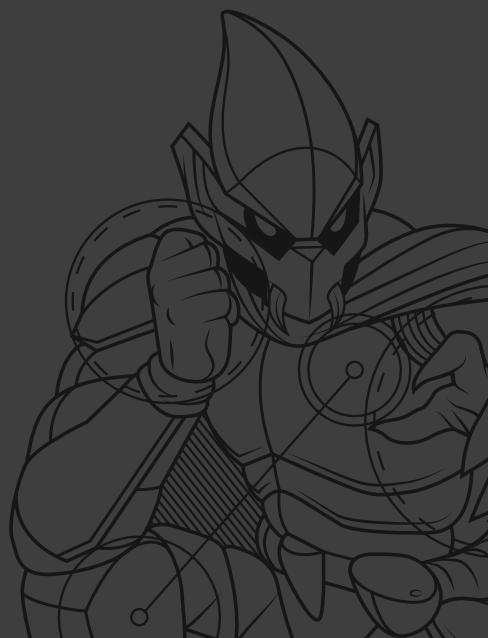
» 数日かかっていた攻撃の分析を数分で完了

» お客様のより正しい判断を支援

» お客様が受けた攻撃の背景を完全理解

» クラウド型ですぐに使える

» カスタマイズされたIOCで他のセキュリティ機器と連携



製品の特徴

1. シンプルな仕組み

- **同一の管理画面で参照可能 ー** Falcon Intelligenceの分析結果は、検出した脅威情報と同じく、CrowdStrike Falconの管理画面の上で表示されます。ここで得られるまとまった十分な情報をもとに、セキュリティ担当者はより迅速で、より正しい判断ができます。
- **脅威情報を直接取得 ー** Falcon IntelligenceはCrowdStrike Falconによって保護されているエンドポイントでブロックされた脅威情報を直接取得し、自動的に分析します。セキュリティ担当者は、チームの規模やスキルレベルにかかわらず、現実の攻撃から学ぶ機会を逃すことはありません。
- **すぐに使えるクラウド型 ー** Falcon Intelligenceの機能は全てクラウド上で構築されていますので、お客様がオンプレミスでハードウェア等をご用意いただく必要はなく、契約後すぐにお使いいただけます。

2. より速く、より効果的な対処が可能に

- **時間、労力、費用の節約 ー** サイバー攻撃の調査の各ステップを自動化したことで、これまで数日かかっていた分析・調査を数分でできるようになりました。Falcon Intelligenceは、マルウェア分析、マルウェア検索、脅威インテリジェンス参照をシームレスなソリューションに統合し、まとまった結果を表示しますので、対策までの時間を劇的に短縮できます。
- **関連する脅威に対する防御 ー** お客様が受けた攻撃と、攻撃者が世界で展開している一連の攻撃キャンペーンや拡散中のマルウェアとを紐付けしますので、経営陣へのより内容の濃い報告が可能です。Falcon Intelligenceは、業界最大のマルウェア検索エンジンを活用して関連する他のサンプルを数秒で検索できますから、それらの関連するマルウェアが侵入していないかの調査も合わせて行うことができます。この手法によって、カスタマイズされたIOCが生成でき、将来の攻撃からお客様を守ることができます。
- **悪質な攻撃者の手口を理解 ー** CrowdStrikeの脅威インテリジェンスによって、攻撃者グループの目的、使用するテクニックやツール、主に狙う脆弱性などを知ることができます。これによって将来の攻撃を防ぐためのプロアクティブな対策が取れるようになります。

3. さらに高度な機能も装備

- **IOCによる防御 ー** 他のネットワークセキュリティデバイスに容易に展開できるIOCを提供。Falconだけが提供できる深い分析結果により、幅広く、かつ関連性の高い一連のIOCを提供します。
- **YARAルールとSuricataルールの生成 ー** 分析結果からYARAルールとSuricataルールを自動生成。従来、専門的スキルが必要だったこれらのルール記述が自動化されることで、どなたでも高度な防御を実装できるようになりました。
- **他のソリューションとの容易な統合 ー** 豊富なAPIとツールにより、既存のセキュリティソリューションとの容易な統合が可能です。

最も速く、最も簡単に脅威をコントロール

検出された脅威をいかに迅速に分析し、迅速な対策を打つかは攻撃から身を守るために不可欠な能力となっています。Falcon Intelligenceはこれまで専門的知識を必要とし、数日かかっていた分析と対策を、誰でも数分で実現できるようにした、画期的ソリューションです。

CROWDSTRIKE

CrowdStrikeは、クラウドベースの次世代エンドポイントプロテクションの業界を牽引しています。CrowdStrikeは、次世代のアンチウィルス、EDR、および24時間体制のマネージド脅威ハンティングサービスを統合し、すべてを1つの軽量エージェントで提供する、業界初、かつ唯一の企業として、革新的なエンドポイントプロテクションを提供しています。

詳細は、crowdstrike.com/sites/jp をご覧ください。

CrowdStrike Japan株式会社
〒100-0005
東京都千代田区丸の内1丁目6-5