CROWDSTRIKE

INCIDENT RESPONSE

概要

CrowdStrike Servicesは、インシデントの事前・事後対応サービスを提供することで、サイバー インシデントに防御と対応力を向上させます。**CrowdStrike**のインシデント対応チームは、全世界で何百もの重大なデータ漏えい調査対応を行っています。実際に発生したインシデントへの対応や復旧の経験と最先端テクノロジーの組み合わせにより、ほぼリアルタイムで攻撃者を検知、追跡を行い、お客様環境への不正アクセスを素早く阻止し、いち早く通常業務に復旧します。

CrowdStrikeは、企業の知的財産や金銭を狙った高度な攻撃者によるインシデントに随時対応しています。弊社のコンサルタントは、国家主導の攻撃者、組織的犯罪集団、ハクティビスト、内部不正によるインシデント対応に精通しています。

主な攻撃者

国家主導の攻撃者	あらゆる規模の企業や政府機関を狙い、知的財産や個人情報（個人識別情報、保護されるべき医療情報など）を盗みます。
組織的犯罪集団	金銭目的で、銀行、小売業者、クレジットカード会社などの金融機関を狙い、金銭、個人識別情報、クレジット／デビットカード情報の搾取や、不正な送金などを行います。
ハクティビスト	政治的・社会的な目的で、企業を狙い、標的企業のイメージ低下や風評被害を目論みます。
内部不正	自らが所属する企業を狙い、復讐、風評被害、競合への機密情報の横流しをします。

方法論／アプローチ

CrowdStrikeは、迅速に包括的なトリアージを行い、標的型攻撃者による不正アクセスを阻止し、不正アクセスが発生した際にお客様自身が必要な対応策が実行出来るようにします。

すべての組織・すべてのインシデントはそれぞれに異なります。お客様と協力し、調査を通じて理解した業務上のニーズ、既存のシステムとリソースを考慮した対応・復旧が必要な項目を作成し、ビジネスとセキュリティニーズの調和されたお客様専用の復旧対応計画を提供します。

最先端テクノロジー

弊社のコンサルタントは、調査にCrowdStrikeのFalcon Platformの検知機能やFalcon Forensicsの機能を取り入れ、組織が迅速に効率的な対応を図ることを可能にします。

Falcon Platformテクノロジーは、攻撃手法に共通するパターン（権限昇格、侵入拡大、認証情報搾取など）をモニタリングするための先見的なデータを継続的に提供し、お客様環境内のエンドポイントにおける不正行為を防ぎます。

Falcon Forensicsは、従来のフォレンジック手法（例えば攻撃の兆候を積み重ねるなど）を通して、お客様のネットワーク内で過去に発生した不正行為を特定できるようにします。このデータを分析することで、経緯が整理され、攻撃者がアクセスした場所や実行した活動内容を適切に評価できるようになります。

CrowdStrike Falconテクノロジーにより、過去の攻撃活動だけでなく、進行中の活動も検知できるようになります。また、業界で最も包括的な可視性やより徹底的な調査を実現し、早急な修復が可能になります。

CrowdStrike Servicesの詳細につきましては、WWW.CROWDSTRIKE.COM/SERVICESをご覧ください。

お客様の声

「私たちの業界は、巧妙な攻撃に集中的に狙われています。弊社のニーズに細かく応えた**CrowdStrike Services**の提供するサービスにより、確実に脅威を予想し、ネットワークを備え、サイバー攻撃からの防御力を向上させることができます。」

- CISO（フォーチュン100に選ばれた金融サービス）

CrowdStrike Servicesによるデータ漏えい防止方法や、標的型攻撃の対策と防御方法につきましては、弊社担当者までお問い合わせください。

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

CROWDSTRIKE