CROWDSTRIKE

COMPROMISE ASSESSMENT

CROWDSTRIKE SERVICES

データ収集・分析と理解

CrowdStrike ® Servicesチームは、大規模で複雑な標的型攻撃を受けた組織のインシデント対応（IR）調査を幅広く行ってきた経験に基づき、現代の極めて先進的な攻撃者の戦術、手法、手順（TTP）について、独自の見解を提供することができます。

こうした知識や専門性に加え、受賞歴を誇るクラウドベースのCrowdStrike Falcon®プラットフォームのエンドポイント テクノロジーを取り入れ、組織のIT環境に対する包括的な侵害診断を行い、「自組織への侵害が発生していないか？」という重要な疑問に答えます。

CrowdStrike Servicesチームの仕事は、従来のように、兆候に基づく検知や特定時点に限られたモニタリングに留まりません。CrowdStrikeのCompromise Assessmentでは、従来のフォレンジックデータに対する専門的な分析と、リアルタイムの脅威検知やハンティングを重視します。過去と現在にエンドポイントで発生した出来事を把握することが、未来のIT環境の防御方法を探るための鍵となります。

CROWDSTRIKEの方法論とアプローチ

CrowdStrikeのCompromise Assessmentは、Microsoft Windows、Mac OS X、また各種Linuxベースのオペレーティングシステムから調査に必要なデータを効率的に収集し、分析するところから始まります。現場に調査用機器を設置することや、脅威の兆候を積極的にかき集める必要はありません。データの収集、分析と同時に、CrowdStrike Falconプラットフォームがリアルタイムで脅威の検知や環境のモニタリングを行い、マルウェアやマルウェア以外の脅威だけでなく、「実際の」不正活動を窺わせる攻撃の兆候（IOA）も探します。

環境内における不正活動の存在を適切に評価するためには、調査に基づき、これまでの経緯を包括的に理解することに加え、動的なモニタリングが不可欠です。すべての環境は異なるため、CrowdStrike Servicesチームは早い段階でお客様と効率的な協力を図り、そのネットワーク トポロジーや感染経路となっているシステムを把握します。CrowdStrike Servicesチームは、こうした情報を基にお客様の環境内で使用するアプリケーションやツールを理解し、活用することができます。

お客様の協力により、CrowdStrikeはお客様にとり正常な活動を判断し、フォレンジック データ収集、ネットワーク モニタリングとサイバーセキュリティ サービス業界で他にはないエンドポイントにおける検知と対応（EDR）を提供します。

実践的な分析と所見

CrowdStrikeは、Compromise Assessmentの成果物は、ITセキュリティやエンタープライズリスク管理部門の関係者全員にとって分析レポートや所見は適切であり行動に結びつかなければならないと認識しています。
CrowdStrikeのコンサルタントが提供する報告書には、以下の項目が含まれます。

- お客様環境を標的とする侵入攻撃の証拠が発見されるかどうか、お客様のセキュリティ体制に対する効果的な改善提案
- 最も重要な発見物、結論、提案事項の要旨
- 発見された問題の修正、除去、検証に必要な情報を盛り込んだ、お客様の技術チーム向けの技術評価
- その他、CrowdStrikeが発見した、リスクの高いコモディティ化されたマルウェア、不審なスクリプトやファイル、リモートアクセス ユティリティ、管理作業など

受賞歴を誇るテクノロジーで迅速な可視化を実現

CrowdStrikeのコンサルタントは、以下のテクノロジーを活用してCompromise Assessmentを行います。

- **Falcon Insight ™** は、CrowdStrikeのエンドポイントにおける検知と対応（EDR）ソリューション。お客様の環境で使用される各エンドポイントに単独の軽量エージェントを導入し、クラウドに特化した高度な保護を提供。

- **Falcon Forensics Collector (FFC)** は、遠隔導入が可能で、各エンドポイント上の45種類以上におよぶフォレンジックデータから情報を収集するクロスプラットフォームの非永続的単測ツール。

- FFCから収集した**フォレンジックメタデータ**は、CrowdStrikeクラウドで集計、処理され、解析や、不正なTTPを追跡や特定するサイバー脅威インテリジェンス「CrowdStrike Falcon Intelligence ™」との相互参照が可能。

CrowdStrikeのコンサルタントは、収集したIOAデータの調査、統計的異常の特定（お客様環境全体で不審な処理パターンを特定するなど）、侵入拡大や不審なユーザー振る舞いのトラッキングや追跡、また既知のマルウェアやハッキングツールのハイライトなどを行います。

CrowdStrike Falconプラットフォームは、攻撃パターンを継続的にモニタリングするため、リアルタイムで先見的なデータを提供します。権限昇格、侵入拡大、マルウェア展開、認証情報のダンピングなどの不正行為は直ちに検知することができ、後続の攻撃活動による感染からお客様のエンドポイントを守ることができます。

さらに可視性を向上させる必要がある場合は、CrowdStrike のFalcon Network Sensorテクノロジーによって、お客様のネットワークへの出入口を監視し、潜在的に不正な通信を検知することができます。Falcon Network Sensorは、ネットワークトラフィックを受動的に取得、分析、切断し、CrowdStrike Falcon Intelligenceやお客様企業独自の検知パターンに基づき、不審な通信について警告を発行するステルス技術です。FFCやFalconプラットフォームのデータと同様、Falcon Network Sensorテレメトリも CrowdStrikeクラウドのインフラ内で集計され、CrowdStrikeの経験豊富なネットワーク セキュリティ モニタリング（NSM）ハンターによって分析されます。

CROWDSTRIKEで情報漏えいを防止:

WWW.CROWDSTRIKE.COM/SERVICESをご覧ください。

CrowdStrike Servicesが提供する標的型攻撃の防御サポートの詳細につきましては、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