CROWDSTRIKE

エンドポイント リカバリサービス

事業を中断せずAPT攻撃から迅速に回復

時間との闘い

侵害行為が発生した場合に事業への影響を最小限に抑えるには、修復と回復までのスピードが非常に重要です。APT攻撃（Advanced Persistent Threats：持続的標的型攻撃）はネットワークを一瞬で突破し、エンドポイントに感染して、システムに広がって事業を混乱させます。

このように巧妙で持続的なサイバー攻撃は、多くの場合、システムにマルウェアを感染させたり、長期間にわたって機密データを盗んだりすることを目的として、検出されない持続的なポイントをネットワーク内にいくつも確立します。こうした攻撃は、綿密に計画・設計され、組織に入り込んで既存のセキュリティ手法の隙を狙って、目立たないように実行されます。ここで最も重要なことは、適切で効果的な対策をして持続的なポイントをすべて取り除くことです。そうしないと最初に修復した後も攻撃者がシステムを再感染させ、事業の回復が遅れて中断が長引く原因となります。

迅速な回復の必要性

侵害行為が発生した場合には、セキュリティチームが迅速で正確な意思決定をすることが、攻撃から回復し、影響を最小限に抑えて通常のビジネスプラクティスを再開するためのポイントになります。現在、非常に巧妙な各種の攻撃が存在しているため、適切なアプローチでなければ　検知できません。また、攻撃を検知しても、組織内で混乱が起きることがあります。知識や経験が不足しているセキュリティチームでは、このようなタイプの有害なマルウェアを阻止しようとして、無駄な時間を消費することになるためです。

CrowdStrike®のエンドポイントリカバリサービスは、テクノロジ、インテリジェンス、専門知識を適切に組み合わせて提供し、既知のセキュリティインシデントの検知、分析、修復をサポートし、事業を中断せずに迅速な回復を可能にします。CrowdStrikeのソリューションは、侵入行為の発生後、数時間で展開できるため、短時間で事業を回復することができ、攻撃者が再び現れないことを確信できます。

主なメリット

すぐに攻撃を阻止する：CrowdStrike Falcon®プラットフォームをすばやく展開し、脅威そのものを即時に根絶し、以降に環境へ侵入しようとする試みを未然に防ぎます。

短時間で環境を回復する：悪意のあるアーティファクトや継続的なベクターをすばやく特定し、まとめて修復することで、環境が再び脅威に晒されないようにします。修復にかかる時間は平均72～96時間です。

事業の混乱を最小限にする：事業を効率よく効果的に回復します。各種デバイスのイメージを再適用したり、再支給したりする必要はありません。

回復費用を削減する：平均で数週間～数か月かかっていた回復期間が数日間に短縮されます。中断がないため、事業をすぐに回復できます。

継続的なサポートを提供する：回復期間（通常は最初の72～96時間）の後も、セキュリティの脅威に対してCrowdStrike Servicesが引き続き監視し、対処します。

リカバリエンゲージメントの主なフェーズ

CrowdStrikeのエンドポイントリカバリサービスは、30日間単位で利用でき、ネットワーク内のエンドポイントの迅速な回復を可能にします。エンゲージメント期間中、CrowdStrikeはFalcon　OverWatch™チームのセキュリティに関するグローバルな専門知識を用いて環境を監視し、新たな攻撃や、攻撃が繰り返されることを予防します。

予防

- エンゲージメントの最初の24時間以内に、Falconプラットフォームを迅速に展開および構成して、検知を開始します。強力な予防ポリシーで、アクティブな攻撃の実行とラテラルムーブメント（侵入拡大）を即時に阻止します。

回復

- 次の72～96時間で、CrowdStrike Servicesチームが Falconプラットフォームを利用して攻撃を分析し、積極的に修復を行い、メモリに残留しているマルウェア、持続しているその他のアクティブな攻撃のコンポーネントを除去します。
- CrowdStrike　Servicesチームは、Falconコンソール内で特定されたセキュリティイベントに基づいて提案を行います。攻撃インテリジェンスと分析対象のデータポイントを組み合わせることにより、考えられる原因、攻撃のテクニック、脆弱性について見解が得られます。これで回復が可能になり、以降の攻撃を防ぐことができます。
- エンゲージメントでは、事業を混乱させずにエンドポイントをすばやく効率的に回復させ、フォレンジック調査を回避することに焦点をおいています。

監視

- CrowdStrikeは、システムが回復した後もサービスエンゲージメントの残りの期間は、以前のインシデントが再発しないか、継続して環境を監視し、新たなインシデントやネットワークへの侵入の試みを検知して修復します。
- OverWatch脅威ハンティングチームは、最強のセキュリティテクノロジでさえも通過するような攻撃テクニックが出現していないかを監視します。攻撃者の動きが観測され、修復が必要な場合は、回復チームに直接連絡します。

レポート

- サービスエンゲージメントの終了時に、回復チームが最終レポート（エグゼクティブ向けのサマリーと技術的な説明）を提供します。この最終レポートでは、エンゲージメント期間中に行われた監視、分析、回復の活動を総括します。

CROWDSTRIKEについて

CrowdStrike®Inc.（ナスダック：CRWD）は、サイバーセキュリティ市場をけん引するグローバル企業で、侵入行為を阻止するために新しく構築したエンドポイント保護プラットフォームにより、クラウド時代のセキュリティを再定義しています。CrowdStrikeFalcon®プラットフォームの非常に軽量なエージェントアーキテクチャは、クラウド規模の人工知能（AI）を利用し、企業全体をリアルタイムに保護、可視化することで、ネットワークの内外を問わずエンドポイントへの攻撃を予防します。独自のCrowdStrikeThreat Graph®を備えたCrowdStrike Falconは、世界中で1週間に発生する3兆件以上のエンドポイント関連イベントをリアルタイムで相互に関連付けるもので、世界で最も高度なセキュリティ用データプラットフォームの基盤の1つです。

CROWDSTRIKEが選ばれる理由

CrowdStrikeは、エンドポイント保護およびインシデント対応の分野におけるリーディングカンパニーです。テクノロジ、インテリジェンス、専門知識を適切に組み合わせて提供し、侵入行為のすばやい検知、攻撃の調査、攻撃者の排除、エンドポイントの修復により、混乱を最小限に抑えて、攻撃からの回復を可能にします。

最先端のテクノロジプラットフォーム：クラウドネイティブなFalconプラットフォームを数時間で展開し、攻撃をすばやく検出および調査することで、ご利用の環境から攻撃者を排除します。

インテリジェンスによる修復：CrowdStrikeのグローバルな脅威インテリジェンスは、最新のIOA（IndicatorsofAttack：攻撃の痕跡）とIOC（Indicators of　Compromise：侵害の痕跡）を利用し、環境内で検知されずに活動している可能性のある、非常に巧妙で持続的な脅威も検知します。

サイバーセキュリティの専門知識：CrowdStrikeのセキュリティ分析では、長年の経験と専門知識を活用し、ウィルスなどに感染したエンドポイントと直接やりとりして、残留しているすべてのアーティファクトと持続的なメカニズムを取り除くことにより、再感染を予防します。マシンのイメージを再適用する必要はありません。

迅速な回復：市場をリードするCrowdStrikeのエンドポイントテクノロジ、グローバルな脅威インテリジェント能力、そして卓越したセキュリティ専門知識があれば、最も巧妙な攻撃や持続的な脅威から環境を回復させることができるため、事業を迅速に回復できます。