CrowdStrike Services

CROWDSTRIKE

CROWDSTRIKEの インシデント対応サービス およびプロアクティブサービス

攻撃に対する
訓練、対応、回復を
迅速かつ効果的に実施

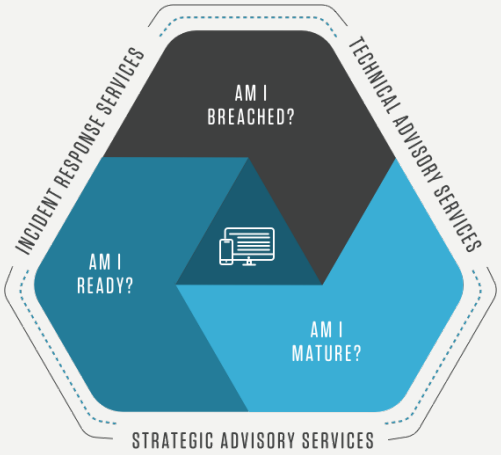
CROWDSTRIKEのインシデント対応サービスおよびプロアクティブサービス

要望に合わせてサービスを選択

CrowdStrike® Servicesには、インシデント対応（IR）とプロアクティブなサービスの両方が含まれます。これらは、組織がセキュリティ対策を成熟させ、侵害を阻止するうえで極めて重要な役割を果たします。これらのサービスは、組織がサイバーセキュリティインシデントに迅速かつ効果的に対応できるように支援します。更に、お客様は総合的なサイバーセキュリティ対策の強化をするために設計された、多様なプロアクティブサービスも活用できます。

CrowdStrike® Servicesでは、このサービスを提供するために、情報機関、法執行機関、セキュリティ業界からセキュリティのプロフェッショナルを、世界中の最高レベルのテクノロジー企業からはアーキテクトやエンジニアを結集しています。また、世界で最も困難な侵入調査を指揮してきたセキュリティーコンサルタントもチームに加わっています。

同チームは、CrowdStrike Falcon®プラットフォームを幅広く活用して画期的なエンドポイントプロテクションを実現し、リアルタイムのインシデント対応、詳細なフォレンジック分析、および脅威インテリジェンスを可能にして、脅威が監視をすり抜けることがないようにしています。CrowdStrike® Servicesは、さまざまなセキュリティインシデントや高度なサイバー攻撃に対する計画、対応および被害の防止に努める組織を支援することに秀でています。特に、将来的な攻撃への防御支援には優れた実績があります。



CrowdStrikeのインシデント対応サービスとプロアクティブサービスは、個別に利用することも、組み合わせて利用することも可能です。これらは、リテイナー契約でカバーされ、柔軟にサービスを組み合わせて提供されています。インシデント対応サービスは必要ないとお考えであれば、リテイナー契約の時間をプロアクティブサービスに使用していただくことができます。これらのサービスでは、組織の全体的なセキュリティ体制の強化を支援することに注力しています。

CROWDSTRIKE SERVICESの概要

CrowdStrike® Servicesのサービスは、次の3つの基本的な問いに答えることにより、組織のセキュリティ体制の強化と成熟を支援します。

侵害を受けたか？

- インシデント対応サービス
- エンドポイント修復サービス
- 侵害調査サービス
- ネットワークセキュリティ監視

セキュリティ体制の成熟度は十分か？

- サイバーセキュリティ成熟度評価
- Active Directoryセキュリティ評価
- クラウドセキュリティ評価
- SOC評価
- ITハイジーン評価
- サイバーセキュリティ強化プログラム
- セキュリティ詳細プログラム

攻撃に対する準備はできているか？

- 机上演習
- ライブファイヤー演習
- 攻撃者エミュレーション演習
- レッドチーム/ブルーチーム演習
- ペネトレーション・テスト・サービス

マネージド型のサービス、サポート、トレーニング

- Falcon Complete™
- Falconオペレーションサポート
- Falcon トレーニング（CrowdStrikeユニバーシティ）

CROWDSTRIKEのインシデント対応サービスおよびプロアクティブサービス

侵害を受けたか？

インシデント対応サービス

- 攻撃者の活動を包括的に把握することで、侵害発生後の修復を加速し、ビジネスオペレーションを迅速に再開できるようにします。CrowdStrikeのインシデント対応サービスは、組織と協力して重大なセキュリティインシデントに対応します。フォレンジック分析を行って、サイバー攻撃後の迅速な収束を支援し、長期的なソリューションを実行して再発防止に努めます。
- CrowdStrikeのインシデント対応チームは、クラウドベースのユニークなFalconプラットフォームを活用して、実世界におけるインシデント対応、フォレンジック調査、および修復の経験を最先端のテクノロジーと組み合わせ、インテリジェントベースのアプローチを用いて対応策を講じ、迅速かつ正確に攻撃者を特定して環境から排除します。同チームは、組織を迅速に業務に復帰させ、サイバー攻撃の影響を軽減することに力を注いでいます。

エンドポイント修復サービス

- CrowdStrikeエンドポイント修復サービスは、ビジネスの中断を生じさせることなく、高度な標的型攻撃からの迅速なリカバリーを支援します。
- このサービスでは、業界をリードするCrowdStrikeのテクノロジープラットフォームと脅威インテリジェンス機能を、経験豊富なセキュリティ・エキスパートのチームと組み合わせて、既知のセキュリティインシデントの検知、分析、修復を支援し、迅速なリカバリーを可能にします。

侵害調査サービス

- CrowdStrikeの侵害調査サービスチームは、現在または過去に組織の環境内で発生した攻撃者の活動を特定し、「我々は侵害を受けたのか？」という重大な問いに答えます。
- 侵害調査サービスチームは、非常に高度な攻撃者の侵入に対処してきた長年の経験を活かし、強力なFalconプラットフォーム、業界をリードするサイバー脅威インテリジェンス、24時間365日体制の脅威ハンティング機能を組み合わせて、お客様の環境におけるセキュリティ侵害を包括的に評価します。

ネットワークセキュリティ監視

- このサービスでは、広範なネットワークセキュリティ監視機能を提供し、環境内で活動中の脅威を検知します。
- この監視機能を活用して、攻撃の検知、対応および脅威ハンティングを実行します。このサービスは、CrowdStrike® Servicesの脅威ハンターチームの専門知識と、環境内に存在する脅威を検知するネットワークアプライアンスの両方をもって実現しています。

CROWDSTRIKEが選ばれる理由

実績ある専門家：インシデントレスポンダー、マルウェアリサーチャー、サイバーインテリジェンスのプロたちが迅速なインシデント対応、フォレンジック分析、エンドポイントリカバリー、プロアクティブなサービスを提供。

アドバーサリーインテリジェンス：企業環境を狙う攻撃者とその戦術、技法、手順に関する最新の調査結果を活用できる。

無敵の脅威ハンティング：プロアクティブな24時間年中無休のハンティング機能が環境全体における攻撃者の活動を広く捜索。

優れたテクノロジー：CrowdStrike Falcon®独自のプラットフォームで提供される次世代型のエンドポイントプロテクション機能で、攻撃者を検知してすばやく排除する。

CROWDSTRIKEのインシデント対応サービスおよびプロアクティブサービス

セキュリティ体制の成熟度は十分か？

サイバーセキュリティ成熟度評価

- CrowdStrike® Servicesは、「コンプライアンスを確保」していても安全であるとは限らないと主張しています。Servicesチームは、コンプライアンスだけに焦点を当てるのではなく、脅威に長年対処してきた経験から得た鋭い観察眼をもって、組織の成熟度を評価します。
- Servicesチームが用いる手法は、標準的な監査の域を超えるものです。非常に高度な攻撃を回避、検知、対応する組織の能力を測り、サイバーセキュリティ上の成熟度を評価します。

Active Directoryセキュリティ評価

- Active Directory（AD）の構成とポリシー設定に関する包括的な評価を提供することにより、ADインフラストラクチャーの悪用を防止することができます。
- CrowdStrikeのActive Directoryセキュリティ評価は、ADの構成とポリシー設定を確認し、攻撃者に悪用されかねないセキュリティ構成の問題を特定するために設計された独自の機能です。
- このアセスメントでは、ドキュメントのレビュー、担当者とのディスカッション、専用ツールの実行、およびADの構成と設定の確認が行われます。その結果、発見された問題とその影響に関する詳細レポートに加え、問題の改善と修正のための推奨手順が提供されます。

クラウドセキュリティ評価

- CrowdStrikeのクラウドセキュリティ評価では、セキュリティ上の設定ミスや、推奨されるクラウド・セキュリティ・アーキテクチャーからの逸脱に関する実用的な知見が提供されます。
- インシデント対応におけるCrowdStrikeの経験を活用し、クラウド・セキュリティ・アーキテクチャー業界のリーダーとして実践的な経験を積んだコンサルタントが実施するこのアセスメントでは、クラウド内で発生するセキュリティインシデントの予防、検知、復旧機能を最大限に強化するために必要となる優先順位付けされたアクションを提供します。

ITハイジーン評価

- 侵害が発生する前に、脆弱性を事前に検知し、ネットワークを保護します。
- CrowdStrikeのITハイジーン評価では、ネットワーク内のアプリケーション、アクセシビリティ、およびアカウント管理の可視性が強化され、ネットワークトラフィックとセキュリティギャップに関する包括的なコンテキストが提供されます。脆弱性や未適用のパッチを特定することで、侵害が発生する前にネットワークをプロアクティブに保護できます。

サイバーセキュリティ強化プログラム

- 侵害の発生後にサイバーセキュリティ強化プログラムを開発・実施して、セキュリティギャップを解消し、さらなる侵害を防止します。
- CrowdStrikeのサイバーセキュリティ強化プログラムは、最近セキュリティ侵害を受け、新たなセキュリティ侵害の発生を防止するための戦略的なサイバーセキュリティ強化計画の策定を必要としている組織を支援します。

その他のサービス

SOC評価：SOCの成熟度レベルを向上させ、改善すべき領域を特定し、優先順位付けを行う。

セキュリティ詳細プログラム：サイバーセキュリティのためのプロセス、ツール、リソースを詳細に調査し、情報セキュリティプログラムの成熟度を判断する。

脅威インテリジェンスプログラム開発：進化する脅威の環境、グローバルな攻撃者グループ、および最新のTTP（戦術、テクニック、手順）に基づいて、脅威インテリジェンスを管理するプログラムを構築する。

CROWDSTRIKEのインシデント対応サービスおよびプロアクティブサービス

攻撃に対する準備はできているか？

机上演習

- 高度なサイバー脅威に対するインシデント対応調査を実施し、高度な経験を重ねてきたCrowdStrike® Servicesチームが、机上の演習プロセスに現実に即した視点を提供します。
- 演習は、標的型攻撃をシミュレートするように設計されており、組織の幹部や技術者は現実的なインシデントシミュレーションを行えます。この演習では、業務の中断や損害を生じさせることなく、攻撃を体験できます。

ライブファイヤー演習

- この演習は、インシデント対応シナリオにおいて、組織内の個人がそれぞれの役割を理解しているかをテストする目的で設計されています。
- Servicesチームは、仮想的な攻撃についてグループで話し合うのではなく、お客様の組織のツールとプロセスを活用して現実性を高め、実際の侵害調査時と同様に、具体的な情報を特定の個人に提供します。そのうえで、どのように情報を管理するのがベストなのかをお客様に判断していただきます。最終的には、組織のプロセスの欠点をはっきりと理解できるようになるでしょう。

攻撃者エミュレーション演習

- この演習には、実際のインシデントで生じるような損害を受けることなく、高度な標的型攻撃を経験できるという利点があります。
- 演習では、経験豊富なCrowdStrikeのコンサルタントが、組織のネットワークにアクセスして特定の資産を侵害しようとする最近の攻撃手法を模倣します。攻撃が成功すると、Servicesチームはどのように目的を達成したかを説明し、組織が将来的な攻撃回避に向け戦略を立てられるよう支援します。

レッドチーム/ブルーチーム演習

- 企業環境内で攻撃側（レッドチーム）と防御側（ブルーチーム）に分けた攻撃演習を行い、企業のサイバーセキュリティチームの準備体制を整え、専門家から学ぶ機会を提供します。
- CrowdStrikeのレッドチーム/ブルーチーム演習は、実世界の標的型攻撃シナリオを通じて、組織のセキュリティチームの脅威ハンティングの知識と全体的なインシデント対応プロセスを成熟させることを主な目的としています。

ペネトレーション・テスト・サービス

- Servicesチームは、組織のシステム、ネットワーク、アプリケーションなどの各コンポーネントに対して、攻撃シミュレーションやペネトレーションテストを実行して倫理的なハッキングを行うことにより、セキュリティ上のギャップを特定します。
- さまざまなテストオプションから、御社のセキュリティ上の目的に合致するものを選択してください。

マネージド型のサービス、サポート、トレーニング

- **FALCON COMPLETE™：**この包括的なエンドポイントプロテクションおよび脅威ハンティングソリューションは、Falconプラットフォームのパワーを活用し、ターンキー方式の完全なマネージドサービスとして提供されます。
- **FALCONオペレーションサポート：**オペレーショナルサポートは、Falconプラットフォームの設定と管理を支援し、サイバーセキュリティオペレーションを最適化します。
- **FALCONトレーニング（CrowdStrikeユニバーシティ）：**プロフェッショナルによるトレーニングとCrowdStrikeユニバーシティ（CSU）の教育サービスは、サイバーセキュリティチームの知識を強化し、Falconプラットフォームへの投資を最大限に活用するうえで役立ちます。

CROWDSTRIKE SERVICESについて

CrowdStrike® Servicesは、セキュリティインシデントの防御と対応に必要な保護策と専門知識を企業に提供します。CrowdStrike® Servicesチームは、クラウドベースのCrowdStrike Falcon®プラットフォームを活用して、次世代型のエンドポイントプロテクション、サイバー脅威インテリジェンスの収集・報告、24時間365日のプロアクティブな脅威ハンティングを行うことにより、お客様がリアルタイムで攻撃者を特定、追跡、ブロックできるよう支援します。CrowdStrikeはその独自のアプローチで、不正なアクセスをただちに阻止して侵害の拡大を防ぎます。さらに、CrowdStrikeが提供するプロアクティブなサービスにより、組織は脅威を予測し、ネットワークのセキュリティ体制を整え、最終的には侵害を阻止できるようになります。

www.crowdstrike.jp/services/
で詳細をご覧ください。

Eメール:
services@crowdstrike.com