

Cisco Breach Protection Premier

安心運用、将来を見据えたセキュリティの構築、価値実現までの時間の短縮

Cisco Breach Protection Suite は、脅威の検出、調査、緩和、ハンティングの各ソリューションを 1 つにまとめたものです。エンドポイント、電子メール、ネットワーク、クラウド向けのシスコのセキュリティ製品と厳選されたサードパーティツールを統合しています。ただし、すべての組織がこのソリューションを導入して管理する能力や専門知識を備えているわけではありません。マネージドサービスは、まさにこうしたニーズにお応えするものです。

Cisco Breach Protection Premier は、お客様とお客様のチームの現状に合わせて対応します。現在導入されているツールとテレメトリソースを活用し、シスコの比類のない専門知識とガイダンスを適用して、お客様が全体的なセキュリティ戦略に厚みを持たせ、ソリューションを拡張、追加される際に、お客様とともに成長していきます。

Cisco Breach Protection Premier

Cisco Breach Protection Premier ライセンス階層では、シスコのセキュリティ専門家からなる精鋭チームによる Managed Extended Detection and Response (MXDR) 機能が提供されます。これには、シスコのセキュリティソリューションの統合サポートと、シスコが厳選したサードパーティセキュリティツールとの統合、Cisco Software Support サービス (SWSS) Enhanced サポート、シスコテクニカルセキュリティアセスメント (CTSA) によるセキュリティ評価、検証、強化、および Talos インシデント対応チーム (Talos IR) の厳選サービスが含まれます。

Cisco Managed Extended Detection and Response (MXDR) サービスは、シスコの研究者、調査員、対応担当で構成される精鋭チームと、Cisco XDR ソリューション、統合ツールセット、および追加のシスコセキュリティテクノロジーを組み合わせて使用し、潜在的なセキュリティの脅威と侵害をモニターして対応します。

Cisco XDR を活用する MXDR サービスには、次のものが含まれます。

- ・ シスコのセキュリティオペレーションセンター (SOC) を通じて、イベントとアラートのセキュリティインシデントを 24 時間 365 日体制で常時モニタリング。
- ・ MXDR SOC アナリストが、プラットフォームデータの分析、すべてのイベントの関連付け、強化、優先順位付け、レビューを担当。定評のあるハンドブックを活用して行います。
- ・ 必要に応じて潜在的なセキュリティインシデントをエスカレーション。
- ・ 脅威を封じ込め、軽減、低減、または根絶するためのガイドラインに基づく対応措置。事前に承認された対応ハンドブックに基づいて、お客様に代わって調査と対応を実施します。

- ・ 四半期ごとの報告会。現在の脅威パターン、検出量、トレンドとなっているイベントに関する最新情報を提供します。
- ・ 新たに発見された脅威を特定する脅威アドバイザリ。緩和策を導入することによってインシデントをプロアクティブに防止するのに役立ちます。

CTSA は、一連のプロアクティブなサービススイートを通じてお客様のサイバーセキュリティ整備状況を評価し、お客様が直面している脅威、脅威が現実のものとなる可能性、そうなった場合お客様の業務回復力にどのような影響があるかについてアドバイスを提供します。以下はサービスの一例です。

- ・ 脅威のモデリング/緩和/シミュレーション
- ・ ペネトレーションテスト (ペンテスト)

- ・ レッド/ブルー/パープルチーム演習
- ・ セキュリティ アーキテクチャ アセスメント
- ・ アプリケーション/SOC/DevOps アセスメント
- ・ ビルド/コンフィグレビュー

Talos IR は、サイバーセキュリティ インシデントへの備えと対応、およびサイバーセキュリティ インシデントからの復旧を支援する、フルスイートのプロアクティブサービスと緊急サービスを提供します。

Talos IR と CTSA のサービス時間は、対象ユーザー (CU) 用に購入された Cisco Breach Premier ライセンスの数に応じて決まります。追加時間は、Talos IR および CTSA のアラカルトオフアワーを通じてご購入いただけます。

シスコが提供するマネージドサービスをご利用になれば、安心して運用し、将来を見据えてセキュリティを構築し、価値実現までの時間を短縮できます。

詳細はこちら：cisco.com/jp/go/breach-protection

サービス	最小時間
オンデマンドでのインテリジェンス提供	5
侵害リスク評価ワークショップ	5
組織のデジタル フットプリント アセスメント	10
セキュリティデザイン思考ワークショップ	20
緊急インシデント対応*	40
ペネトレーションテスト	40
脅威モデリング	40
デバイス設定およびビルドのレビュー	40
IR 計画	50
IR ハンドブック	50
机上訓練	50
セキュリティ アーキテクチャ アセスメント	80
IR 準備アセスメント	80
侵害評価	80
サイバーレンジ	80
プロアクティブな脅威検出	100
レッドチームによる脅威シミュレーション	160
パープルチーム演習	160
セキュリティ運用アセスメント	160

* 20 ~ 39 時間のお客様は、限定的な緊急インシデント対応サービスをご利用いただけます。