SOPHOS

Managed Threat Response (MTR)

専門家による脅威対応

Sophos MTR (Managed Threat Response) とは、脅威ハンティング、検出、対応機能を年中無休でソフォスの専門家チームより提供するフルマネージド型サービスです。(ご注意、現時点では英語による対応となります。)

主な特長

- 高度な脅威ハンティング、検出、対応機能をフルマネージドサービスとして提供
- 年中無休の対応チームと共同して、リモートから脅威を封じ込め、無力化するアクションを開始
- MTR 部門が実行するアクションとインシデントの管理方法の決定および制御
- 業界トップレベルの機械学習と経験豊富な専門家から構成されたチームの組み合わせ
- 2種類のサービス (Standard と Advanced) より、あらゆる規模の企業に対して広範囲な機能を提供しています。

脅威通知は解決にはなりません - そこからすべてが始まります

新たな脅威を積極的に防御しつつ、セキュリティプログラムを年中無休態勢で効果的に管理する適切なツール、人材、プロセスを社内に持っている企業はほんとどありません。単に攻撃や疑わしい挙動を通知するだけではなく、Sophos MTR チームは、お客様に代わって標的を絞った行動を開始し、最も洗練され複雑な脅威さえも無効化します。

Sophos MTR の使用で、年中無休態勢で脅威ハンターや次のようなレスポンス専門家のチームにより守られます。

- 潜在的な脅威とインシデントをプロアクティブに追跡し、検証する
- 利用可能なすべての情報を使用し、脅威の範囲や重大度を判定する
- 有効な脅威に対して適切なビジネスコンテキストを適用する
- 脅威をリモートから阻止、封じ込め、無力化するアクションを開始する
- 再発するインシデントの根本原因に対処するための動作のアドバイスを提供する

人による対応を加速させる機械学習

Sophos MTR は Intercept X Advanced with EDR テクノロジーに基づいて、向上した脅威ハンティングと検出、より詳しいアラートの調査、および迅速で正確に脅威を排除するように標的を絞った行動に対して、機械学習と専門家の分析を融合しています。常に業界トップレベルのソフォスのエンドポイント保護と高度な EDR 機能を、最高レベルのセキュリティ専門家のチームとの融合で、「Machine-Accelerated Human Response (人による対応を加速させる機械学習)」というものが生まれました。

完全な透明性と制御

Sophos MTR は、いつ、どのようなタイミングで潜在的なインシデントをエスカレーションし、どのような対応アクション (もしあれば) を当社に希望し、そして誰をコミュニケーションに含めるかなどをお客様で決断し、制御することができます。
Sophos MTR は３つの対応モードの機能があり、MTR チームはインシデント中にお客様と共に最善の方法を選択できます。

通知: ソフォスは、検出した脅威についてお客様に通知し、緊急度を特定して問題の解決を支援します。

共同対処: ソフォスは、お客様の社内担当者または外部の担当者と共同して、検出した脅威に対処します。

承認: 脅威の封じ込めおよび除去は当社で行い、実行したアクションについてお客様に通知します。

Sophos MTR サービスレベル

Sophos MTR は、2種類のサービス (Standard と Advanced) があり、あらゆる規模の企業に対して広範囲な機能を提供しています。選択したサービスレベルに関係なく、組織は独自のニーズに合わせて 3つの対応モード (通知、共同作業、承認) のいずれかを利用できます。

Sophos MTR : Standard

年中無休のリード主導 (手掛かりがある) の脅威ハンティング

確認された悪意のあるアーティファクトやアクティビティ (強力なシグナル) を自動的にブロックまたは終了し、脅威ハンターの負担を軽減し、手がかりをもとにリード主導の脅威ハントを実行できます。このタイプの脅威ハントでは、以前は検出できなかった新しい攻撃の指標 (IoA) と感染の痕跡 (IoC) を発見するための因果的および隣接するイベント (弱い信号) のアグリゲーションと調査が行われます。

セキュリティ状態のチェック

Intercept X Advanced with EDR から始めて、動作状況と推奨される構成の改善を積極的に調査することで、最高のパフォーマンスで Sophos Central 製品を稼働させ続けます。

アクティビティレポート

ケースアクティビティの概要により、優先順位付けとコミュニケーションが可能になり、各レポート期間内でどのような脅威が検出され、どのような対応が実行されたかを把握できます。

攻撃を検出

成功する攻撃のほとんどでは、監視ツールで正当と思わせるプロセスを実行します。ソフォスは独自の調査手法を使用して、正当な動作と攻撃者が使用するTTP (戦術、技術、攻撃手順) との違いを判断します。

Sophos MTR : Advanced すべての Standard 機能に加えて、以下の機能となります。

年中無休のリードレス (手掛かりなし) の脅威ハンティング

データサイエンス、脅威インテリジェンス、およびベテランの脅威ハンターの直感を適用して、企業プロファイル、価値の高い資産、リスクの高いユーザーを組み合わせ、攻撃者の行動を予測し、新しい攻撃の指標 (IoA) を特定します。

テレメトリーの強化

エンドポイントを超えて拡大される他の Sophos Central 製品からのテレメトリで脅威調査を補完し、持続的攻撃の全体像を提供します。

プロアクティブな対策改善

セキュリティ対策をプロアクティブに改善し、全体的なセキュリティ機能を低下させる構成とアーキテクチャの弱点に対処するために、規範的なガイダンスを使用して防御を強化します。

専用の脅威対応リード

インシデントが確認されると、専用の脅威対応リードが提供され、アクティブな脅威が無力化されるまで直接オンプレミスリソース (社内チームまたは社外パートナー) と連携して取り組みます。

直接連絡サポート

セキュリティ オペレーション センター (SOC) へ直接連絡できます。MTR 運営部門は世界26か国にわたり年中無休態勢でサポートします。

アセットの検出

OS のバージョン、アプリケーション、脆弱性をカバーするアセット情報から、マネージドアセットとアンマネージドアセットの識別までをカバーし、影響の評価中、脅威ハント実施中、プロアクティブな対策改善の推奨事項の一環として、分析情報を提供します。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2019-09-17 DS (GH)

SOPHOS