Sophos Rapid Response

アクティブな脅威への迅速な対応

Sophos Rapid Response は、インシデントに対応する専門チームにより、組織に対するアクティブな脅威の特定と無効化を迅速に支援します。(日本語翻訳サービス[翻訳チームによる三者間対応が可能]での提供あり)

攻撃中は一刻が勝負

アクティブ脅威に対応する場合は、最初の感染の痕跡から完全に脅威を軽減するまでの時間をできるだけ短くすることが不可欠です。キルチェーンを進むにつれて、犯罪者の目的を達成することができないようにするには時間との戦いです。

Sophos Rapid Response を使用すると、24 時間 365 日体制で次のことができるリモートインシデント対応チーム、脅威アナリスト、脅威ハンターにより、危険な領域からお客様を迅速に救います。

- アクティブな脅威を優先順位付け、封じ込め、無効化するための措置を迅速に実行
- お客様の資産のさらなる損害を防ぐために組織から脅威を追放
- 24時間365日の継続的な監視と対応を行い、保護を強化
- 根本原因に取り組むためにリアルタイムの予防措置を推奨
- ソフォスのクラウドベースのテクノロジースタックを組織全体に迅速に導入
- サードパーティテクノロジーからの補足データを分析
- ソフォスの調査を説明するインシデント後の脅威の詳細を要約したものを提供

Sophos Rapid Response の機能

Sophos Rapid Response には、Sophos Managed Threat Response Advanced のすべての利点に加えて、その他多くの利点が含まれています。

	Sophos Rapid Response
「承認」脅威のレスポンスモードでの MDR Complete	✓
脅威の監視、ハンティング、対応を24時間年中無休で実施	✓
アクティブ脅威とダイレクトコールアクセス中の専用の対応リード	✓
サードパーティテクノロジーからの補足データを分析	✓
見積もりの迅速化と同日のアカウントの有効化	✓
調査の詳細が把握する正式なインシデント後の脅威の概要	✓

主な特長

- アクティブな脅威を迅速に特定し、無効化
- インシデント対応と 24時間 365 日の監視を 45日間実施
- 専用の連絡先と対応リード
- 実行されたすべてのアクションを詳細に示したインシデント後の脅威の概要
- 固定費および追加料金なしのため、価格設定が予想可能
- 保険料の払い戻しが可能な設計
- Sophos Rapid Response の後、Sophos Managed Detection and Response (MDR) を使用してサブスクリプションにシームレスに移行

SOPHOS

アクティブな脅威の無効化

Sophos Rapid Response チームは、アクティブな脅威を無効化する専門家です。セキュリティ制御を回避しようとしている感染、侵害、アセットの不正アクセスのいずれであっても、ソフォスはすべてを確認し、阻止してきています。

ソフォスの優秀なインシデント対応チームは、Sophos Managed Detection and Response (MDR) の一部です。24 時間 365 日体制の脅威ハンティング、検出、対応サービスにより、フルマネージド型サービスの一環としてお客様に代わり積極的に脅威をハンティング、特定、調査、対応します。

連動したインセンティブ

従来のインシデント対応 (IR) サービスは、1時間単位で価格が設定されているため、脅威を完全に軽減するのに必要な時間を低く見積もるリスクがあります。これでは、追加の時間を購入する必要性が生じます。さらに悪いことに、従来の IR サービスを奨励し、対応にかかる時間を最大限にします。

Sophos Rapid Response は、お客様の組織内のユーザー数とサーバー数によって決定される、追加コストが発生しない固定料金モデルを提供します。また、リモートで提供されるため、初日から対応アクションを開始できます。時間がコストの原因になることはないので、ソフォスはできるだけ迅速に危険な領域からお客様を連れ出すことを優先しています。

Rapid Deployment

可能な限り迅速な対応を実現するために、ソフォスの rapid deployment プロセスでは、Sophos MDR エージェントを検出可能なエンドポイントやサーバーに迅速に配布することに重点を置いています。

既存製品の置き換えのために、取り外し可能なユーティリティを利用した交換戦略を策定した後、リモートで展開するエンジニアチームが、Rapid Response のお客様と相談しながら、ネットワーク全体に大量展開するための自動化ツールを活用して、カスタムプランの行動計画を実行します。

チームは協力して、ネットワーク全体の Sophos MDRe エージェントのセキュリティ状態を最適化し、調査を迅速に行うためのベストプラクティスの設定を確保します。

Rapid Response の使用方法

Rapid Response が承認され、お客様がサービス利用規約に同意した後、すぐにお使いいただけます。Rapid Response には、オンボーディング、トリアージ、無効化、監視の主に 4つのカテゴリーがあります。

オンボーディング

- ホストのキックオフコールで通信設定を確立し、どのような修復手順 (もしある場合) がすでに実行されているかを確認
- 攻撃の規模と影響を特定
- 対応計画を相互に定義
- サービスソフトウェアの導入を開始

トリアージ

- 運用環境を評価
- 既知の感染の痕跡や悪意のあるアクティビティを特定
- データ収集を実行し、調査活動を開始
- 応答アクティビティを開始するための計画を共に作成

無効化

- 攻撃者のアクセスを削除
- アセットやデータへのさらなる損傷を停止
- さらなるデータの流出を防止
- 根本原因に取り組むためにリアルタイムの予防措置を推奨

監視

- MDR Complete サービスへの移行
- 継続的な監視を実行して、再発を検出
- インシデント後の脅威の概要を提供

脅威の概要の詳細

お客様の組織のアクティブな脅威を無効化したら、ソフォスは調査の正式な概要をお客様に提供します。それは、将来似たような脅威の再発を軽減する方法に関する長期的なガイダンスを提案することに加えて、実行したアクション、検出した事項の詳細となります。

インシデント発生後 24時間体制で監視と対応

インシデントが解決され、組織に対する差し迫った脅威が無効化された瞬間に、お客様を最高レベルの MDR サービスである MDR Complete に移行し、24時間体制のプロアクティブな脅威ハンティング、調査、検出、対応を提供します。

脅威が再発、または新たな脅威が出現した場合は、ソフォスは追加費用なしで対応いたします。45日間攻撃を受けている場合は、サブスクリプションの期間中 45日間お客様を保護します。

アクティブな侵害を受けていますか？

以下の地域の番号へ連絡をすることで、いつでもインシデントアドバイザーと話すことができます。

オーストラリア +61 272084454

カナダ +1 7785897255

フランス +33 186539880

ドイツ +49 61171186766

イタリア +39 02 873 17993

英国 +44 1235635329

米国 +1 4087461064

スウェーデン +46 858400610

もし、すべてのインシデントアドバイザーが電話に出られない場合は、メッセージを残してください。すぐに折り返しご連絡いたします。

アクティブな侵害を受けていますか？

詳細は、次のサイトを参照してください。
sophos.com/rapidresponse

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-11-24 DS-JP (DD)