Sophos Compromise Assessment

ビジネスに影響が及ぶ前に侵害の証拠を検出

昨年、企業はセキュリティ侵害の検出と復旧に平均で 37日、240万ドルを費やしました。インシデントレスポンスの専門家チームが提供する Sophos Compromise Assessment は、お客様の環境内で進行中または過去の攻撃者のアクティビティを特定する最も迅速かつ効果的な手段であり、組織は迅速かつ決定的な行動を取ることができます。

アクティブまたは最近の攻撃者アクティビティを特定

Sophos Compromise Assessment は、脅威ハンターとインシデント対応の専門家で構成される専門チームによって提供され、攻撃者がお客様の防御を侵害したかどうかを迅速に特定し、組織のリスクレベルを定量化し、脅威を排除するために必要なアクションについて詳細なガイダンスを提供します。

Sophos Incident Response (IR) サービスチームは、今日の最も高度な脅威への豊富な経験を活用して、侵害の可能性のある資産の対象を絞った調査を通じて、感染の痕跡 (IOC) を特定することができます。その結果、迅速かつ徹底した評価が可能になり、組織は業務効率を維持しながらリスクとコンプライアンスを管理できるようにします。

Sophos Compromise Assessment の流れ

Sophos IR サービスチームは、Compromise Assessment (侵害評価) の各フェーズを通じて、組織との直接的なコミュニケーションを維持し、脅威、リスクエクスポージャー、およびインシデントの解決と根本原因に対処に必要なアクションを明確にします。

1. **最初の調整コール** – この評価は、潜在的な脅威に関する情報の効率的な情報交換、主要な連絡先の特定から始まり、その後に展開範囲や調査プロセスの確認をします。
2. **調査ツールの導入** – 受賞歴のあるクラウド配信ソフォスプラットフォームのガイド付きインストールにより、指定されたデバイス上のデータをすぐに取得し、Sophos IR サービスチームがデバイスのセキュリティ状態を徹底的に評価できるようにします。
3. **脅威の調査とリスク評価** – アクティブな脅威が確認された場合、Sophos IR サービスチームは、お客様の主要な担当者とアクティブな脅威コールを直ちに実施し、広範囲なセキュリティインシデントのリスクと緊急の措置について話し合います。
4. **サマリーコールと書面によるレポート** – 攻撃者のアクティビティの証拠、リスクエクスポージャー、脅威の排除と根本原因への対処に関するガイダンスを詳細に記載した技術文書と非技術的なエグゼクティブサマリーを受け取ります。

Sophos Compromise Assessment の 4つのフェーズはすべて、通常、最初のコーディネートコールから 7日以内に完了します。

主な特長

- 攻撃者が環境内で検出されない状態で動作しているかどうかを迅速に特定
- 広範なセキュリティインシデントの潜在的なリスクを定量化
- 調査の各フェーズで、脅威ハンターやインシデント対応スペシャリストの専門家チームと直接コミュニケーション
- 攻撃者の活動、リスクエクスポージャー、脅威の排除と根本原因への対処に関するガイダンスの包括的な分析を提供
- リスク管理とコンプライアンスのイニシアチブ、ならびに M&A 活動に伴うデューデリジェンスの取り組みを支援

SOPHOS

迅速で徹底的な調査

Sophos Compromise Assessment は、次のような攻撃者のアクティビティを完全に調査し、特定します。

- 疑わしいネットワークアクティビティ
- ラテラルムーブメント
- 異常なファイルまたは悪意のあるファイル
- 自動化されたマルウェアの実行
- 不正アクセス
- 権限昇格
- 防衛回避
- 認証情報窃取
- データ窃取
- 検証されていないスクリプト

評価後

Sophos IR サービスチームが、攻撃者が防御を侵害し、データとビジネスを危険にさらしていることを確認した場合、Sophos Rapid Response への優先オンボーディングのオプションがあります。この完全なインシデントレスポンスサービスは、お客様の IT 環境全体でアクティブな脅威のトリアージ、封じ込め、無力化を実現します。24時間年中無休のリモートインシデント対応担当者が迅速に行動し、お客様の環境から攻撃者を排除し、根本原因に対処するための予防策をリアルタイムで提案します。

侵害の兆候が見つからない場合は、Sophos MDR (Managed Detection and Response) は、24時間年中無休の継続的な検出と対応サービスによって組織を強化することができます。24時間体制の脅威ハンターと対応エキスパートチームが、潜在的な脅威やインシデントを積極的に探し出し、検証します。チームは、進化する脅威の阻止、封じ込め、無力化するためのアクションを継続的に実行し、インシデントの根本原因に対処して、セキュリティの予防策を向上させるための実用的なアドバイスを提供します。

アクティブな侵害を受けていますか？

Sophos Rapid Response を使用すると、24 時間 365 日体制で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。オンボーディングが数時間以内に開始され、ほとんどのお客様は 48時間以内に優先順位付けされます。アクティブな脅威が発生している場合は、次にある地域電話番号に電話して、インシデントアドバイザーにいつでもお気軽にお問い合わせください。

アクティブな脅威が発生している場合は、Rapid Response チーム rapidresponse@sophos.com にメールを送信するか、次の地域番号に連絡してください。

米国：+1 4087461064

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

英国：+44 1235635329

スウェーデン：+46 858400610

イタリア: +39 02 947 52897

オーストリア: +43 73265575520

スイス: +41 445152286

オランダ：+31 162708600

スペイン：+34 913758065

アクティブな侵害を受けていますか？

Sophos Rapid Response の迅速なサポートを受ける

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2023-06-26 DS-JP (PC)