ソリューションカタログ

Sophos Emergency Incident Response

調査から復旧まで、包括的なフルサービスサポートを提供

アクティブな脅威への即時対応

ビジネスが攻撃を受けているときには、1 秒たりとも無駄にできません。インシデントが発生した際、スピード、効率、そしてさまざまな分野にわたるセキュリティスキルと専門知識が必要になります。また、常に変化する世界的な脅威の状況と、最新の攻撃戦術や手法に関する知識および可視化する機能も必要です。

Sophos Emergency Incident Response は、サイバーセキュリティの緊急事態が発生したお客様を支援し、迅速に評価、封じ込め、状況把握、修正措置を実行します。ソフォスの部門横断的な専門家チームが、長年の経験と知見を活かし、アクティブな脅威の重大度判定、封じ込め、無効化を迅速に行い、攻撃者を排除して損害の拡大を防止します。ソフォスは、数千件におよぶ対応で得た知見を活かし、単にインシデントの根本原因を解決するのではなく、将来の攻撃に対するレジリエンスの強化のための改善策と予防措置を提案します。

防御とセキュリティポスチャのプロアクティブな強化

Sophos Emergency Incident Response は協調的かつ対話型のアプローチを採用しており、お客様のチームと連携して迅速に状況を評価し、必要に応じて脅威を封じ込めて排除し、復旧のための具体的なガイダンスを提供します。ソフォスのチームは、Sophos X-Ops と Counter Threat Unit の研究チームによるデジタルフォレンジック、マルウェア分析、脅威ハンティング、脅威インテリジェンスを提供し、脅威を発見して排除します。ペネトレーションテスターや脅威リサーチャーなど、さまざまな分野の専門家を連携させることで、包括的なリスク軽減と復旧を実現します。

検知と調査

初期対応と調査

可能な限り迅速に対応するため、ソフォスは検出可能なホスト / エンドポイントおよびサーバー等へのエージェントの即時展開に全力を注いでいます。このリモートからのインシデント対応支援により、初期分析のサポート、適切な封じ込め対策の策定、および対応全体での迅速な可視化に必要な追加テクノロジーの決定を支援するフォレンジックデータの取得が可能になります。

詳細な調査

データ取得: ホスト / エンドポイントおよびサーバー、影響を受けたサービス、ビジネスへの影響、その他の攻撃方法。

反復的なフォレンジックと脅威分析： リサーチャー、ハンター、ペネトレーションテスター、アナリストが、脅威の全体像を把握するお手伝いをします。

修復計画の策定： 調査と並行して、修復計画の策定を開始します。

お客様にとってのメリット

- 部門横断的なデジタルフォレンジックとインシデント対応の機能と専門知識でチームを強化します。
- 脅威を完全に把握することで、インシデントの影響と再発リスクを軽減します。
- 可視化を強化し、事実を把握し、適切な対応を決定するための「答え」を素早く導き出します。

攻撃対象領域の削減：ソフォスは、攻撃者に関するインタラクティブな知見を提供することで、セキュリティコントロールの有効性の検証と再侵入ポイント特定を可能にし、包括的にリスクを軽減します。

ランサムウェア身代金の交渉：経験豊富なランサムウェア身代金交渉担当者が、ランサムウェア攻撃者に関する深い知識に基づいて交渉を円滑化し、安全かつコスト効果の高い方法でデータを復旧するためのガイダンスを提供します。

修復

セキュリティの確保と検証

集中的なセキュリティ強化：インシデント対応チームは、攻撃者の再侵入を阻止するための戦術的セキュリティコントロールの強化を支援します。

封じ込め：攻撃者のコマンド & コントロール (C2) を遮断します。

攻撃者の排除：隔離されたネットワークから攻撃者を除去するには、その手口を組織的に排除し、侵害されたドメインをリセットする必要があります。

復旧

システムおよびデータの復旧:ソフォスのインシデント対応チームは、システムの再構築、データのサニタイズ、およびシステムの本稼働再開を支援するため、信頼できるパートナーと連携して、シームレスかつ安全な復旧サービスを提供します。

ホストの検証：業界をリードするエージェントテクノロジーを活用し、復旧したホストが本番環境で利用可能であることを確認します。

フォローアップ

業務継続性の改善

ソフォスは、数千件におよぶ対応事例から得た教訓を活かし、推奨される対応プロセスの改善や、セキュリティトランスフォーメーションロードマップの策定を支援する戦略的推奨事項を提案します。対応終了時には、調査結果をまとめた正式なインシデント報告書を提供します。この報告書には、実施した措置、発見した内容、および類似した脅威の再発を防止するための長期的な推奨事項が記載されています。

インシデント対応にソフォスを選ぶ理由

ソフォスが有する豊富な経験が、すべてのサイバーセキュリティ緊急事態への対応に活かされています。ソフォスは、小規模な単一のシステム侵害から、業務に重大な混乱や支障をもたらす全社的な危機まで、さまざまな業種やインシデントの種類にわたる幅広い組織に、フルサービスのインシデント対応支援を提供しています。

経験豊富なソフォスのインシデント対応チームは、国家、軍、組織のコンピューターセキュリティインシデント対応チーム (CSIRT)、法執行機関、情報機関などの幅広い分野での専門知識と経験を活用しています。チームは、主要なサイバーセキュリティ対策に関する実践的知識と、最前線のインシデント対応、X-Ops および Counter Threat Unit の研究チームによる脅威インテリジェンス、セキュリティテストや評価の結果、セキュリティ分析を組み合わせることで、調査を迅速化し、自信を持って復旧を実現します。

サービスの特長

- アクティブな脅威を迅速に特定し、無効化します。
- テクノロジーを迅速に導入します。
- デジタルフォレンジックデータの収集と分析により、IoC (セキュリティ侵害の痕跡) を特定し、攻撃者の活動を追跡します。
- 脅威ハンティングにより、関連する攻撃者の活動を特定します。
- リモートおよびオンサイトでの技術支援、インシデント指揮、アドバイザリー機能を提供します。
- 一般的なサイバー脅威シナリオから珍しいシナリオまで、経験豊富で認定を受けたグローバルなチームがインシデントに対応します。
- インシデント固有の脅威インテリジェンスと、現在の攻撃手法に関する知見を提供します。
- 専門的なランサムウェア身代金交渉を支援します。
- 実施した措置、発見事項、推奨事項を詳細に記したインシデント後の報告書を提供します。なお、本資料掲載のサービスは地域によって、一部提供していない場合がございます。

現在進行中のセキュリティ侵害がありますか？

以下の地域の番号へ連絡すると、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

オーストリア：+43 73265575520

カナダ：+1 7785897255

フランス：+33 186539880

ドイツ：+49 61171186766

イタリア：+39 02 94752 897

スイス：+41 445152286

英国：+44 1235635329

米国：+1 4087461064

日本：0066-33-812-151

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。

Email：EmergencyIR@sophos.com (英語)
日本語をご希望のお客様は、IR-jp@sophos.co.jp までお問い合わせください。

詳細はこちら

sophos.com/emergency-response

ソフォス株式会社
Email: partnersales@sophos.co.jp

2025-06-04 BRJA (MP)