SOPHOS

セールスおよび技術に関する FAQ – Sophos Emergency Incident Response

外部 FAQ

概要

Emergency Incident Response とは何ですか？

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、修正措置の推奨事項を提供します。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。

また Emergency Incident Response は、お客様の組織がインシデントの影響を受けたかどうかを判断し、その影響の範囲を把握するのを支援します。このサービスは、インシデントの根本原因の特定、観測された動作が悪意のあるものかどうかを判断するための侵害評価、脅威ハンティングおよび脅威インテリジェンスの実施、身代金交渉の支援など、さまざまな調査活動を提供します。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。

Emergency Incident Response は誰を対象としていますか？

アクティブなセキュリティインシデントに直面している組織、追加調査が必要な攻撃を最近受けた組織、または脅威となり得るかを判断する上で調査を必要とする活動を検知した組織が対象となります。

Emergency Incident Response を購入するには、ソフォスの既存顧客である必要はありますか？

いいえ。Emergency Incident Response サービスは、ソフォスの既存のお客様とソフォス以外 (ソフォス製品をお持ちでない) のお客様の両方が利用できます。

現在進行形でセキュリティ侵害が発生しています。次に何をすればよいですか？

以下の各地域の番号に電話し、インシデントアドバイザーにご相談ください。

- 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

EmergencyIR@sophos.com までメールでお問い合わせください (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。

Emergency Incident Response はリモートですか、それともオンサイトですか？

リモートとオンサイトのどちらのオプションもご利用いただけます。

Emergency Incident Response サービスはどのくらい迅速ですか？

お客様の大部分は 2 時間でオンボーディングされ、48 時間で優先順位付けされます。このサービスは完全リモートであるため、ソフォスに連絡してから数時間以内に対応が開始されます。

オンボーディングはいつから開始されますか？
Emergency Incident Response チームは、お客様の承認を得るとすぐにオンボーディングプロセスを開始し、調査を始めることができます。

Emergency Incident Response はどのような手法を用いますか？
お客様がサービス契約に同意した後、利用開始のキックオフコールを開催します。ご希望の場合は、メールでの実施も可能です。お客様の目的を把握し次第、調査を開始いたします。

Emergency Incident Response には、さまざまなカテゴリの業務が含まれます。最初のスコープ設定ミーティングにおいて、必要なカテゴリと概算所要時間を一緒に確認いたします。

重点カテゴリには、エンゲージメント管理、インシデント対応、デジタルフォレンジック、侵害評価、脅威ハンティング、脅威インテリジェンスと調査、ランサムウェア身代金交渉、エンゲージメントレポート、オンサイトサポート (該当する場合)、ビジネスメール詐欺 (BEC)、ソフトウェアの展開が含まれます。

Emergency Incident Response はどの言語で提供されていますか？
現在、このサービスは英語と日本語で提供されています。お客様には、技術的な知識を有し、英語または日本語でコミュニケーションできることが求められます。

ソフォスは、データフォレンジックとインシデント対応 (DFIR) サービスと連携していますか、それとも DFIR に代わるものですか？
Emergency Incident Response は DFIR サービスのひとつです。Emergency Incident Response を通じて提供されるサービスのスコープにはデジタルフォレンジックが含まれるため、DFIR 用として別途セキュリティ企業と契約する必要はありません。

ソフォスのテクノロジーをエンドポイントにインストールする必要がありますか？
いいえ。Emergency Incident Response は Sophos XDR を使用して提供できます。または、既存のソリューションと併せて、Sophos XDR センサーを導入することも可能です。どちらを選択しても、インシデントの迅速な調査が可能になります。

Emergency Incident Response チームは、導入が完了するのを待たずに、脅威の封じ込めと無効化のための修正措置を実行できます。チームは、利用可能なデータを活用し、インシデント対応に適したツールを使用します。

価格はどのように設定されますか？
ソフォスは、スコープ設定に関する質問に基づいて、インシデントへの対応に必要な時間を見積もります。お客様は、実際に利用した時間分のみをお支払いいただきます。

追加コストはかかりますか？
オンサイト作業が必要な場合、出張費用はお客様に請求いたします。

Emergency Incident Response を自社環境の一部に導入できますか、それとも環境全体がスコープに含まれている必要がありますか？
特定の状況下では、Emergency Incident Response を環境の一部に適用できます。Emergency Incident Response の専門家が、プロジェクトスコープ決定の一環として詳細をご説明いたします。

ソフォスは、契約上顧客の組織を代表する仲介業者 (法律事務所など) と連携することはできますか？
はい。仲介業者との連携は可能です。

ソフォスは、攻撃で流出した / 盗取されたファイルを特定できますか？
Emergency Incident Response サービスには、攻撃の一部として流出したファイルを特定するためのベストエフォート (最善の努力) が含まれています。ただし、調査の一環として入手可能なデータに依存されるため、このことを保証は出来ません。

ソフォスは顧客の代わりにランサムウェアを復号しますか？
いいえ。これは Emergency Incident Response サービスには含まれていません。

ソフォスは、顧客の代わりに、ランサムウェア身代金支払いの交渉または仲介を支援しますか？
Emergency Incident Response には、サイバー攻撃者とのランサムウェア身代金交渉の専門家による支援が含まれます。ソフォスは身代金支払いの仲介はしませんが、必要に応じて、Sophos MDR または Taegis MDR を活用して、第三者機関を推薦し、連携して対応いたします。

© Copyright 2025.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos は、Sophos Ltd の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

2025-06-03 (WP-NP)