サービスログを使用したフィッシング検知機能の有効性の向上

この章は、次の項で構成されています。

概要

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するためにCisco Talos クラウドサービスに送信されます。

（注） AsyncOS 13.5 以降、サービスログでは Cisco Talos クラウドサービスに送信されるテレメトリデータとして、SENDERBASE が置き換えられます。

Cisco E メール セキュリティ ゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アプライアンスでのサービスログの有効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [サービスログ（Service Logs）] に移動します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [限られた情報をサービスログ情報サービスと共有する（推奨）（Enable sharing limited data with the Service Logs Information Service (Recommended)）] チェックボックスをオンにします。

このボックスをオンにすると、アプライアンスの機能がグローバルにイネーブルになります。イネーブルにした場合、（Cisco アンチスパム スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集にコンテキスト適応スキャン エンジン（CASE）が使用されます。また、CLI の **servicelogsconfig** コマンドを使用して同様の設定を行うこともできます。

ステップ 4 [送信（Submit）] をクリックし、変更をコミットします。

アプライアンスでのサービスログの無効化

手順

ステップ 1 [セキュリティサービス（Security Services）] > [サービスログ（Service Logs）] に移動します。

ステップ 2 [無効化（Disable）] をクリックして変更を確定します。

FAQ

シスコは、プライバシーが重要であると認識しており、プライバシーを考慮してサービスを設計および操作しています。Cisco Talos クラウドサービスに登録した場合は、シスコは組織の電子メールトラフィックに関する集約した統計情報を収集しますが、個人を特定できる情報を収集したり、使用したりすることはありません。シスコが収集した、ユーザまたは組織を特定できる可能性のある情報は、すべて極秘として扱われます。

どのようなデータを共有するのですか。

データは、メッセージ属性の要約情報および Cisco アプライアンスがどのように各種メッセージを処理したかに関する情報です。メッセージの本文すべてを収集するわけではありません。繰り返しになりますが、シスコに提供された、ユーザまたは組織を特定できる可能性のある情

報は、すべて極秘として扱われます（後述のシスコは、共有されたデータがセキュアであることをどのように確認していますか。 （4 ページ）を参照してください）。

次の表では、「人間にわかりやすい」形式でサンプルのログ エントリを説明しています。

表 *1*：電子メールメッセージ情報ごとに共有される統計情報

項目	サンプルデータ
インバウンド SMTP 接続の GUID	0FyIkNX8ThST1 /IdfyNshg==
電子メールメッセージの GUID	1Hss77LIS6u7y5 GDn0QFEQ==
E メール セキュリティ アプライアンス メッセージ ID	5191655
受信者の数とその有効性	1
シスコ以外の Talos エンジン（アンチウイルスや高度なマルウェア防御など）からのスキャナの判定	4
メッセージの処理	MSG_DISP_DROPPED
メッセージの処理理由	MSG_DISP_FILTER
メッセージはアウトバウンド配信用か。	true
メッセージ サイズ	35100
着信メールリレー	true
メールフローの方向	IP_DIR_OUT
AMP 判定情報	file_sha2_256: "\ 217 \ 263 \ 037 \ 004 \ 374`N \3264\265\016\314\227\005E\337\373q \177A\245 \017\004\204\340\231\260!^
ドロップされたメッセージのサンプリング	true

表 *2*：定期的に共有される統計の設定情報

項目	サンプルデータ
アウトブレイクフィルタ機能の有効化	true
送信者ドメインレピュテーション（SDR）無効フラグ	true

項目	サンプルデータ
Context Adaptive Scanning Engine（CASE）のバージョン	3.8.5-036
Talos エンジン	1.95.0.220
有効化された機能の汎用リスト	Sophos_enabled

シスコは、共有されたデータがセキュアであることをどのように確認していますか。

Cisco Talos クラウドサービスへの登録に同意する場合：

- シスコのアプライアンスから送信されたデータは、セキュアなgRPC/HTTP2プロトコルを使用して Cisco Talos クラウドサービスに送信されます。
- お客様のデータはすべて、シスコで慎重に取り扱われます。このデータは、セキュアな場所に保存され、データへのアクセスは、企業の電子メールセキュリティ製品およびサービスの向上またはカスタマーサポートの提供のためにデータにアクセスする必要のあるシスコの従業員および請負業者に限られます。
- データに基づいてレポートまたは統計情報が作成された場合、電子メールの受信者またはお客様の企業を特定する情報が、シスコ以外で共有されることはありません。

データを共有することで Cisco アプライアンスのパフォーマンスに影響はありますか。

シスコは、ほとんどのお客様には若干のパフォーマンス上の影響があると認識しています。IronPort は、電子メール配信プロセスの一環として、既存のデータを記録します。顧客データはアプライアンスで集約され、Cisco Talos クラウドサービスに送信されます。HTTPS を介して転送されるデータの総サイズは、一般的な企業の電子メール トラフィック帯域幅の 1 % 未満と予想しています。

イネーブルにした場合、（Cisco アンチスパム スキャンがイネーブルになっているかどうかに関係なく）データの収集およびデータの収集にコンテキスト適応スキャン エンジン（CASE）が使用されます。

その他ご質問がありましたら、シスコ カスタマー サポートまでお問い合わせください。シスコ サポート コミュニティ を参照してください。

その他の方法でデータを共有できますか。

シスコがより高品質のセキュリティ サービスを提供できるようにするために、ご協力をお考えのお客様のために、追加データの提供を可能にするコマンドを用意しています。このより高レベルのデータ共有では、メッセージに含まれる添付ファイルの明確なファイル名、ハッシュさ

れていないテキスト、および URL のホスト名も提供されます。この機能の詳細について関心をお持ちの場合は、システム エンジニアまたはシスコ カスタマー サポートにお問い合わせください。

その他の方法でデータを共有できますか。