Cisco Advanced Phishing Protection：最初の手順

公開日：2018 年 7 月 22 日

重要なプロジェクト チームのメンバーの確認

- **エグゼクティブ スポンサー**：重要な問題/プロジェクト障害のエスカレーション先です。
- **プロジェクトの所有者**：このプロジェクトの成功に責任を持ちます。
- **プロジェクト マネージャ**：このメンバーは主要な連絡先であり、組織へのインターフェイスとして機能します。また、プロジェクトを合意されたスケジュールに沿って確実に進めること、およびその他の内部グループや部門との協力に責任を持ちます。
- **導入エンジニア**：このメンバーは導入のエキスパートとなり、プロジェクトの主要な技術連絡先にもなります。
- **対象分野のエキスパート**：設計と統合へのインプットを提供する技術リーダーです。決定が組織のビジネス上の戦略に即していることを確認します。
  - メッセージング アーキテクト
  - セキュリティ アーキテクト

最初の Customer Success コールの前に必要な手順

- ユーザ ガイドを確認します。
- e ラーニング ポータルでトレーニング ビデオを確認します。
  - 新しいユーザの作成 - https://cl.ly/qrPd
  - ドメイン タギングのメリット - https://cl.ly/2A1m2w391L1Z
  - 受信トレイのポリシー/ホワイト リスティング - https://cl.ly/1V2w1u463k3e
  - トリガーされたポリシーにより受信者が受信するメッセージを再設定する方法 - https://cl.ly/1v381o3F0K0A

- プラットフォームを使用する、または電子メールのレポートを受信する必要のあるチームメンバーのためにユーザを作成します。

最初のデータ収集

- メールのアーキテクチャとは:環境に最適なセンサー配置を決定するためのエンド ツー エンドのメール フローを示す図を作成します。
  - 次のアーキテクチャ設計のうちいずれか 1 つを選択します。

インライン センサー	インライン設定では、センサーは MTA として機能します。メッセージを受信し、それをネクスト ホップ(通常は別の内部 MTA)に転送する役割を担います。インライン設定を利用するお客様は、センサーによって追加されたヘッダーに基づいて着信メッセージに対するアクションを実行するのにネクスト ホップ MTA を使用できます。
デュアル配信センサー	センサーは基本的に SMTP の「メッセージ シンク」として機能し、電子メール メッセージのコピーを SMTP で受信し、ストリーミング方式でメタ データを抽出します。メッセージ本文と添付ファイルは廃棄されます。SMTP メッセージはセンサーに残りません。デュアル配信は通常、Office365 や G Suite などのホステッド電子メール アーキテクチャを使用します。

  - センサーが組織によってホステッド型として配置されるかオンプレミス型として配置されるかを決定します。
  - DKIM および SPF チェックを現在実行中ですか。実行していない場合、DKIM と SPF の有効化をお勧めします。

これらの認証結果がないとデータ モデリングは調整に時間がかかり、より不完全になることに注意してください。

- センサーのインストールの要件を確認します。
  - センサーのインストール - 第 1 章 https://agari.zendesk.com/hc/en-us/articles/360000659691-Agari-Enterprise-Protect-Admin-Guide
- 保護する重要なユーザまたは重要なグループをキャプチャします。
- この準備作業ガイドを返すとき、質問のメモを取り、自分とのコールをスケジュールするのに最適な時間を提供します。