Cisco Email Security Advanced Phishing Protection v1 – インスタント デモ

最終更新日:2018 年 8 月 9 日

このデモンストレーションについて

このデモンストレーションには、以下の内容が含まれます。

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
• ラップトップ • Google Chrome または Mozilla Firefox ブラウザの最新バージョン • Cisco Advanced Phishing Protection アプリケーションへの URL • Cisco Advanced Phishing Protection アプリケーション用のアカウント	• Cisco AnyConnectR

このソリューションについて

今日のサイバー攻撃者は、ますます高度化する ID 偽装手法を駆使して、各社の従業員に攻撃を仕掛けてきます。しかし、どんな攻撃手法にも、適切なアプローチによって検出できる欠点が存在します。Cisco Advanced Phishing Protection によって、Cisco E メール セキュリティですでに実現されている送信者認証および BEC 検出機能が、さらに補強されます。

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

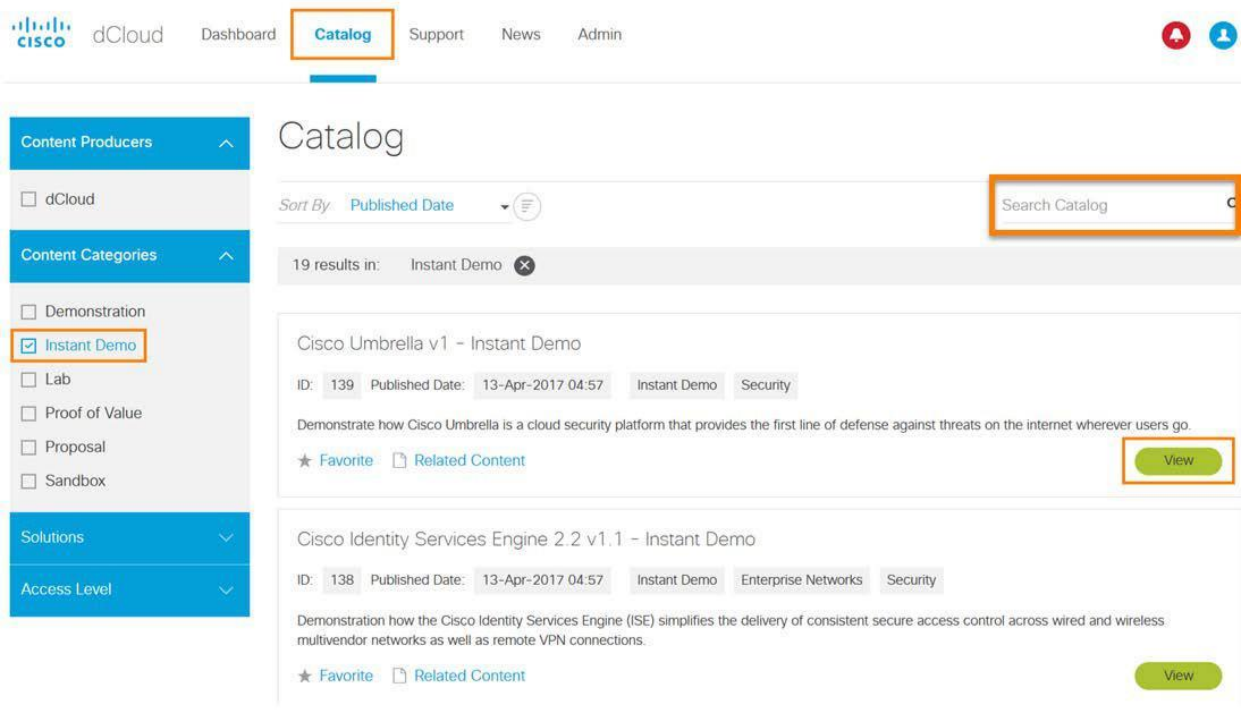
プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. [カタログ（Catalog）] をクリックして、サイド バーから [インスタント デモ（Instant Demo）] を選択します。これで、すべての dCloud インスタント デモが一覧表示されます。
2. 該当する [表示（View）] ボタンをクリックします。

注：または、[カタログを検索（Search Catalog）] ボックスを使用してインスタント デモの名前を検索することもできます。

図 1. インスタント デモ一覧



シナリオ 1.　電子メールの概要

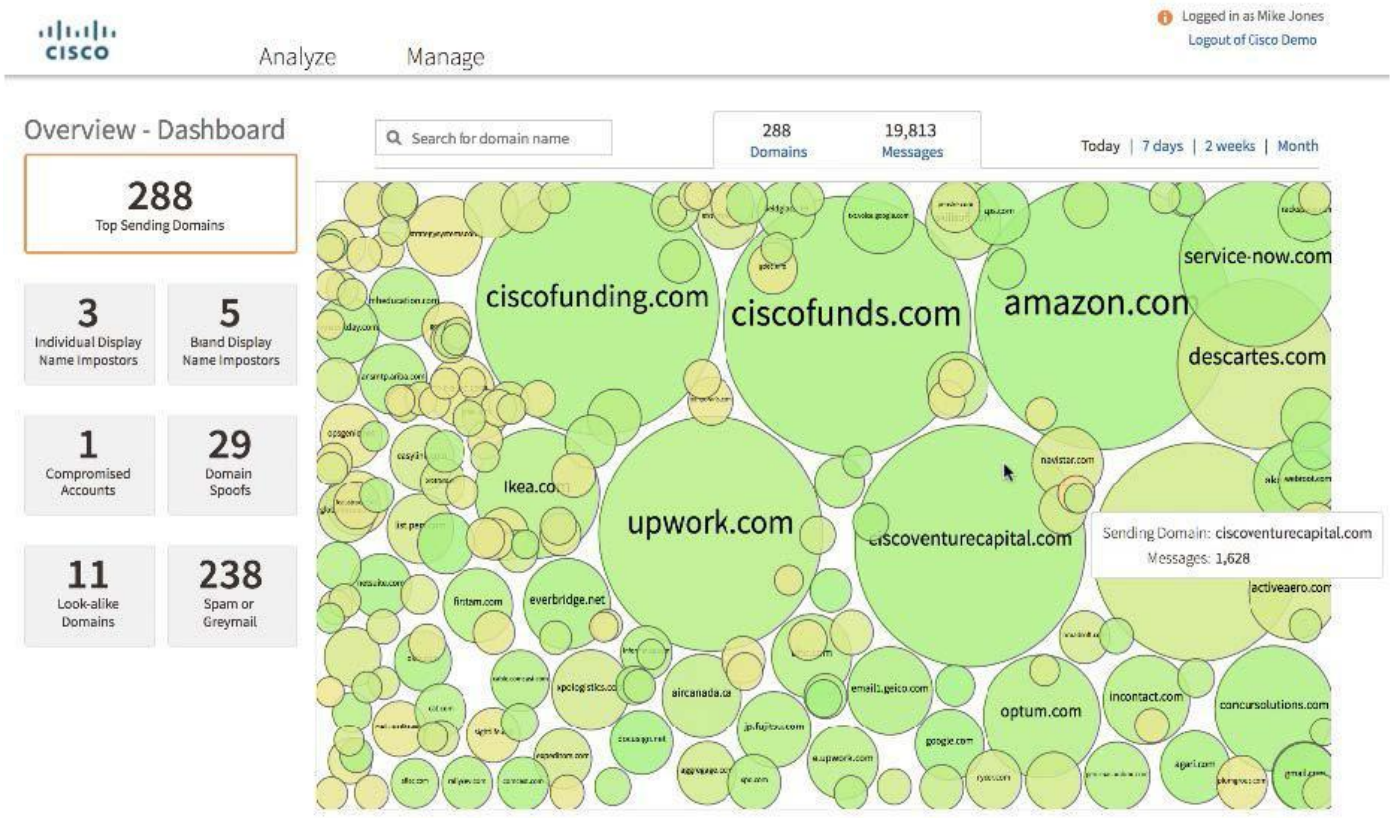
手順

アイデンティティ インテリジェンスは、本物の電子メール送信者の特徴を把握するための重要な情報となります。正当な電子メール送信者は、一貫性のある安定したパターンを示す傾向にあることが判明しています。これを把握して適切にモデル化すると、未知のメールも分類できるようになります。

Cisco Advanced Phishing Protection の [概要（Overview）] ページは、サインインすると最初に表示されるページです。ここには、今日受信した電子メールの概要が図示されています。

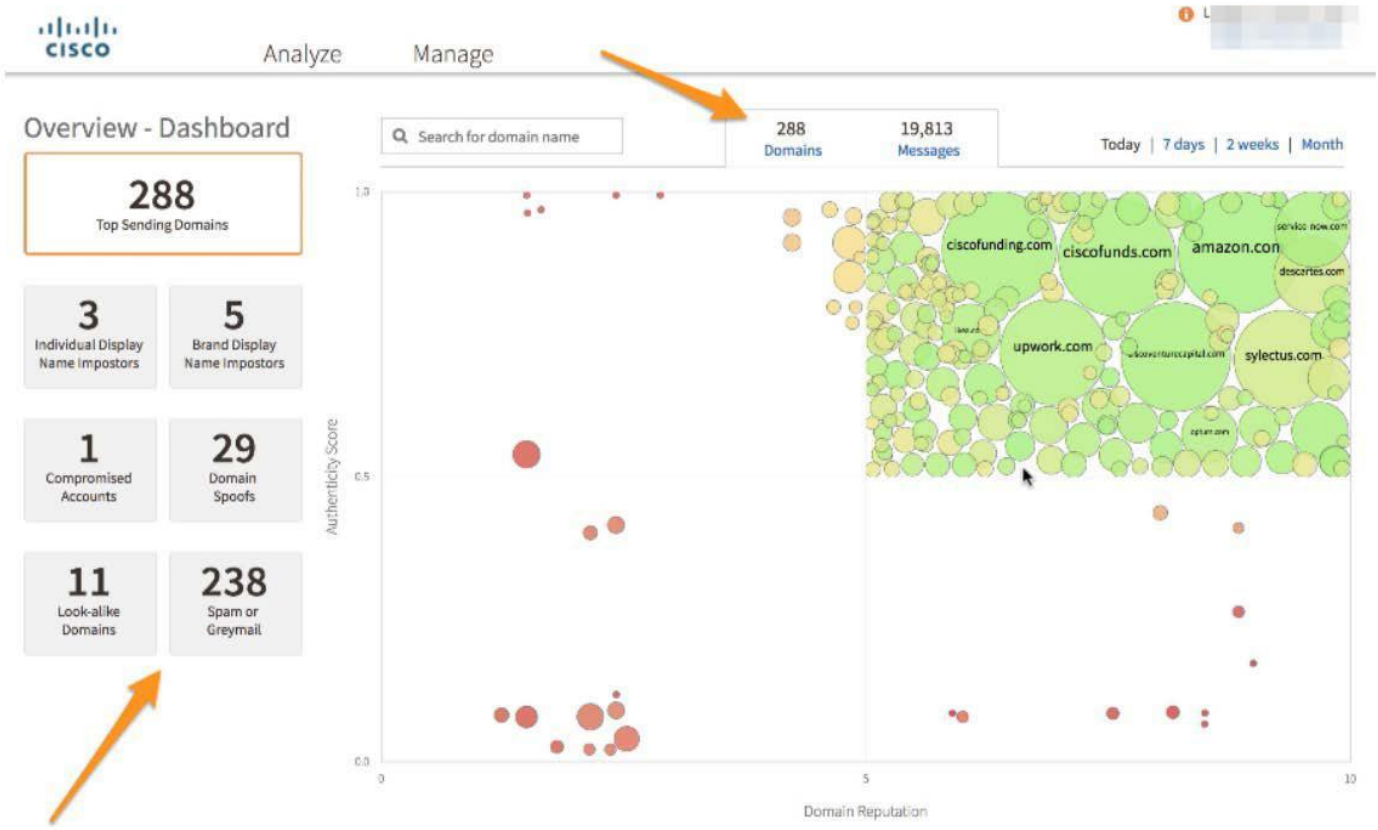
下記に示すのは、私たちの組織が今日受信した電子メールの概要です。

1. 右上の区画の空白部分をクリックすると、その区画が拡大されます。これらは、レピュテーションが高く、正規の電子メールを送信している、安定した正当な送信者です。



右上の区画を拡大すると、そこでは安定した正当な送信者を示しています。信頼できる電子メールが表示される右上の区画に、受信メールの大多数が表示されていることが、一目でわかります。

2. 空白部分をクリックすると、拡大前の表示に戻ります。



また、着信メッセージの送信元ドメインの総数と、受信メッセージの総数の概要も、簡単に把握できます。

左側のタイルでは、Advanced Phishing Protection によって識別された攻撃の種類が、わかりやすく示されています。

上部には、メール送信元ドメインの数と受信メッセージの数が表示されます。攻撃の種類と、それぞれに分類されるメッセージ数が、左側に示されます。

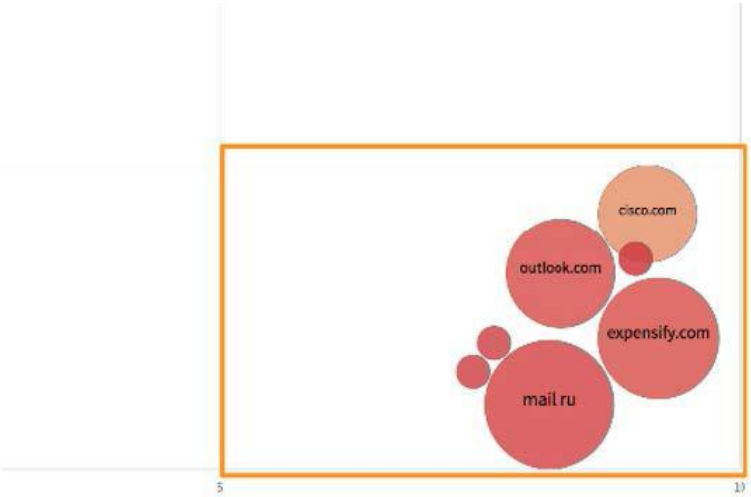
シナリオ 2.　ドメイン スプーフィング

ドメイン スプーフィングとは、攻撃の一種です。このシナリオでは、ドメイン スプーフィングを確認する方法を紹介します。

手順

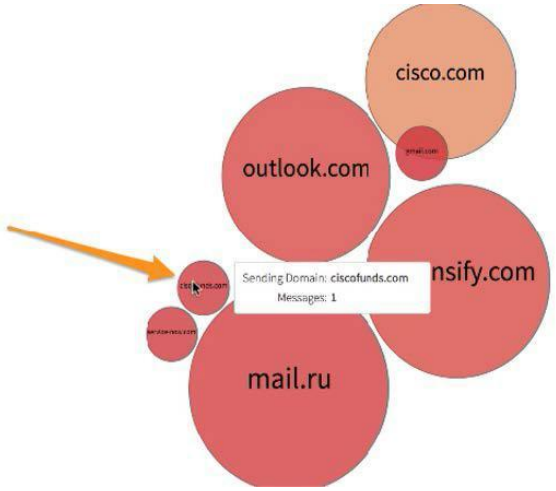
1. [ドメインスプーフィング（Domain Spoofs）] をクリックします。

2. 右下の区画の**空白部分**をクリックします。



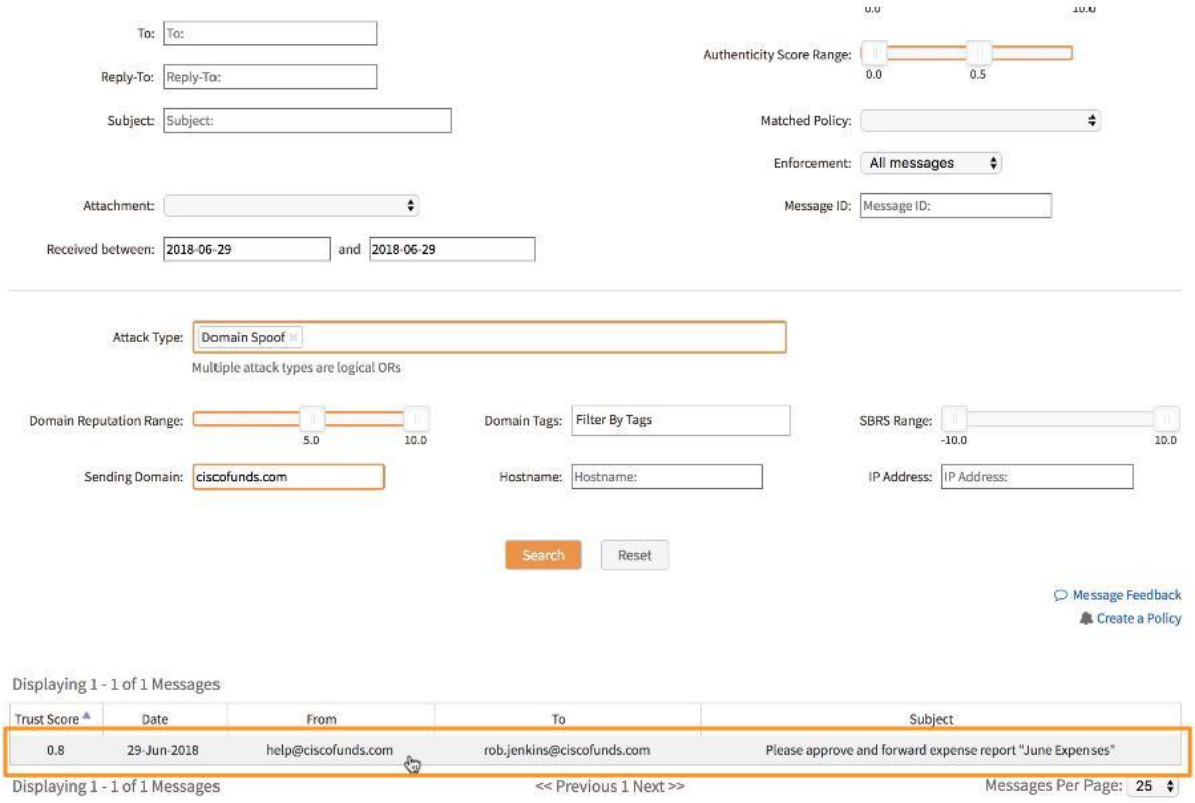
ここに表示されるのは、レピュテーションの高い送信者から着信したとされるメッセージですが、シスコの信頼性モデルに照らし合わせると、見かけと実態が異なる可能性が示唆されます。いずれかの赤い円をクリックすると、一連のメッセージを表示できます。今回は、ciscofunds.com から送信された 1 つのメッセージを見てみることにします。

3. [ciscofunds.com] の円をクリックします。

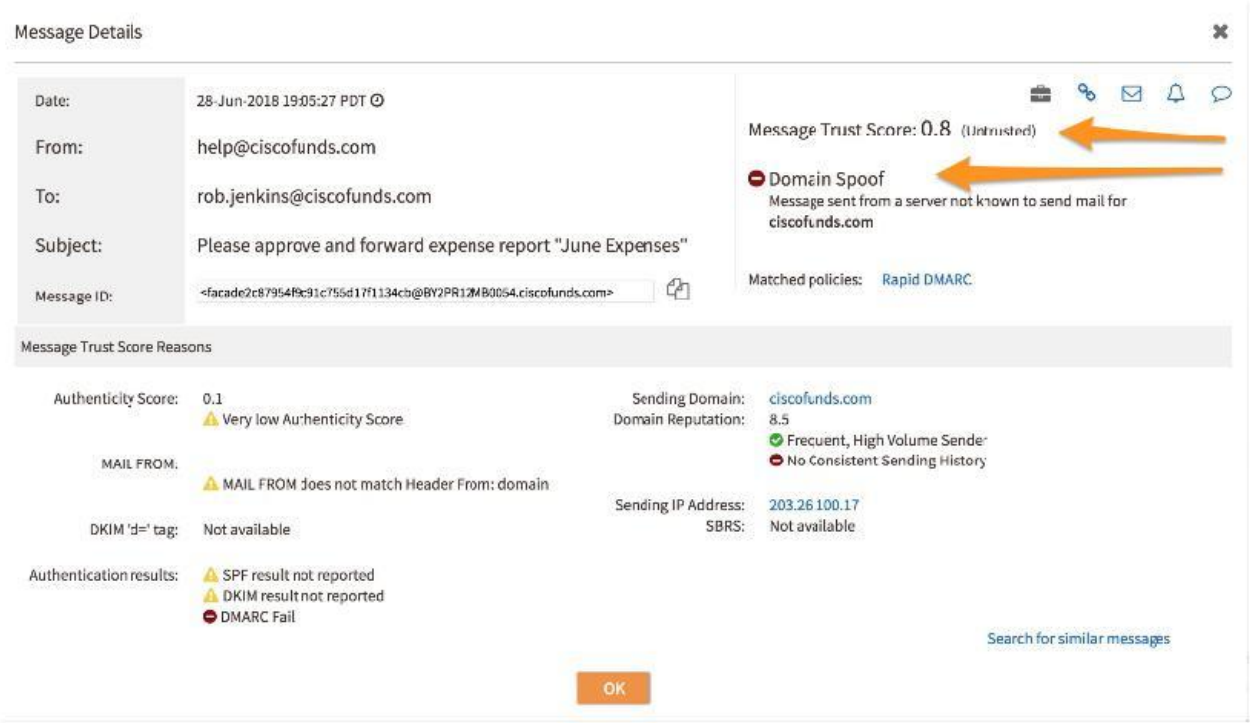


[メッセージの検索（Search Messages）] ビューが表示されます。このビューでのフィルタリング条件は、クリックした円の条件に基づいて、あらかじめ設定されています。

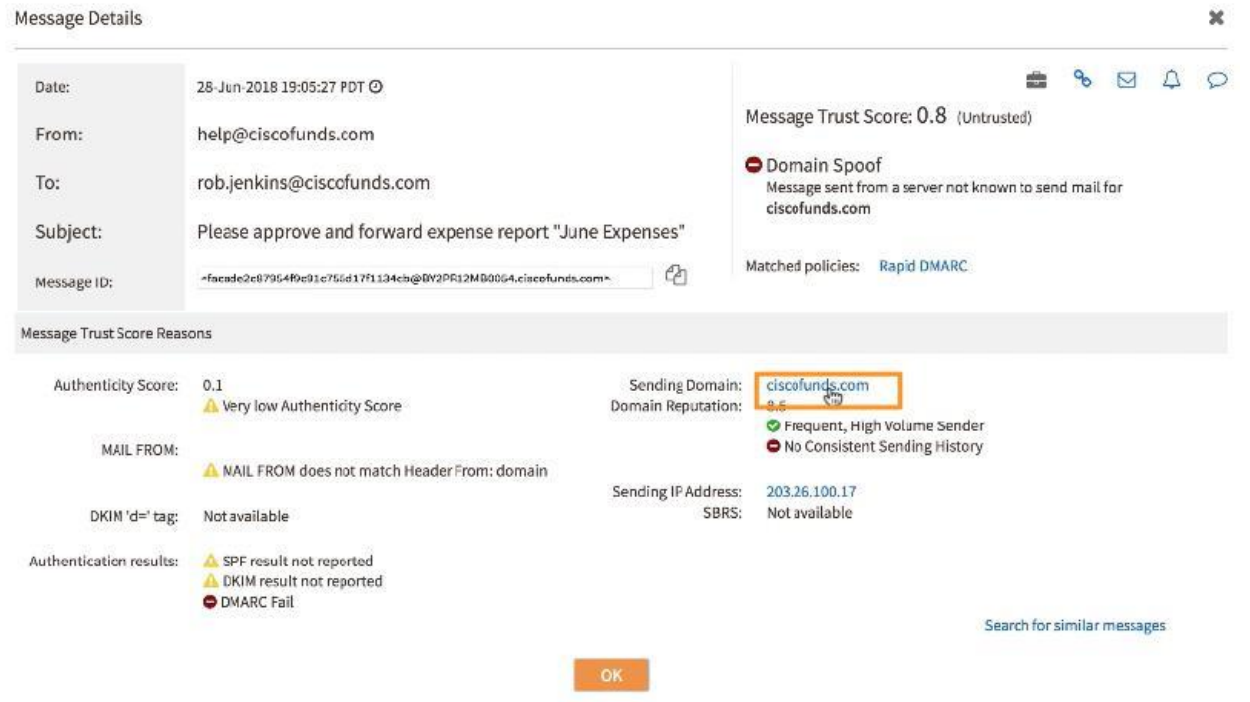
4. **メッセージ**をクリックすると、メッセージの詳細が表示されます。



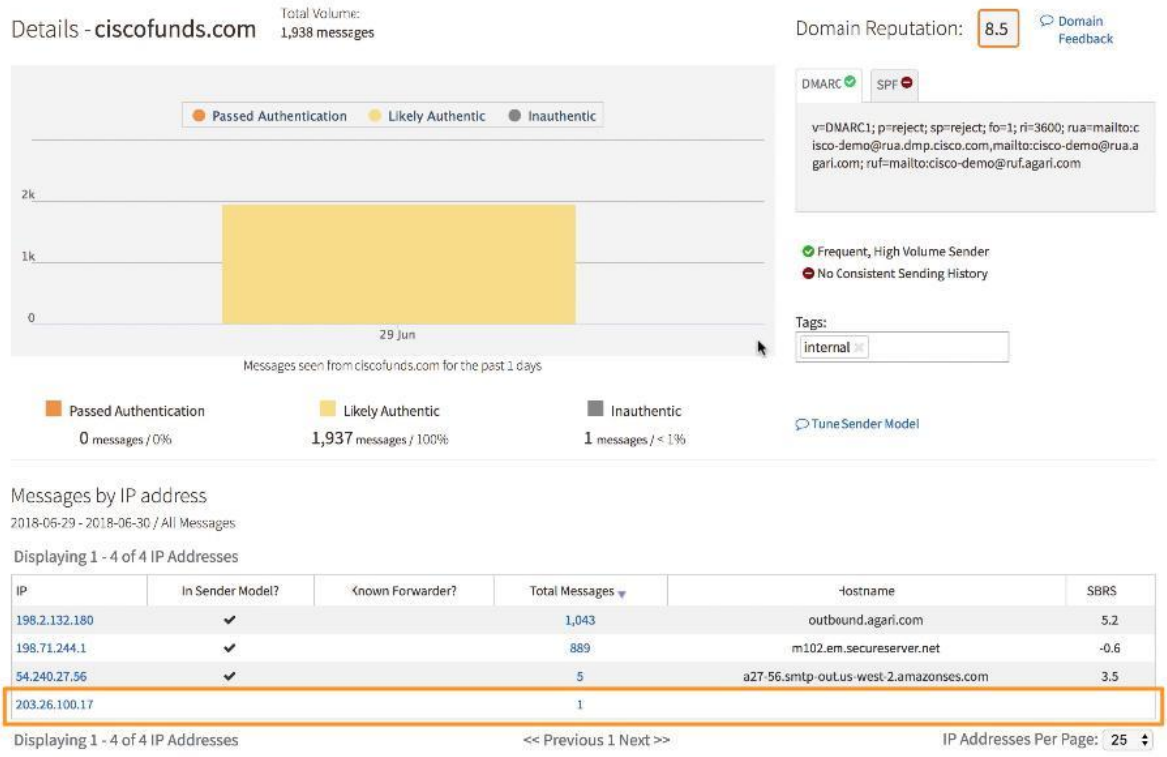
この詳細ビューでは、いくつかのスコアリング モデルの結果を確認できます。右上には、総合的なメッセージ信頼スコアが表示されます。0 ～ 10 点（10 点満点）の中 0.8 点という、非常に低いスコアになっています。このメッセージは、ciscofunds.com への送信元としては未知のサーバから着信しているため、[ドメインスプーフィング（Domain Spoof）] としても識別されていました。



5. ドメイン名である [ciscofunds.com] をクリックすると、このドメインに対する送信パターンが、さらに詳しく表示されます。



このドメイン宛ての正当な送信元 IP アドレスから着信したあらゆるメッセージと比較すると、1 つだけスプーフィング IP アドレスから着信したメッセージが目につきます。



6. シスコのロゴをクリックして [概要（Overview）] ページに戻ります。

シナリオ 3.　アカウントの乗っ取り

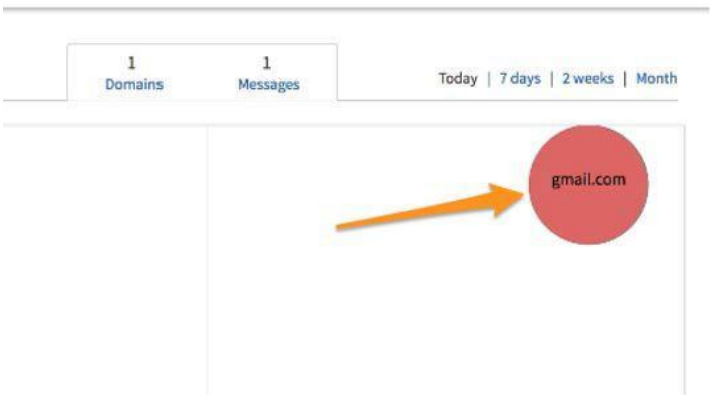
急増している攻撃タイプの 1 つに、アカウントの乗っ取り（ATO）があります。信頼できるドメインのスプーフィングがだんだん困難になってきているため、より複雑な手法に乗り換える攻撃者が増えているのです。Advanced Phishing Protection は、さまざまなタイプの侵害を受けたアカウントからのメッセージを検出および分類します。

手順

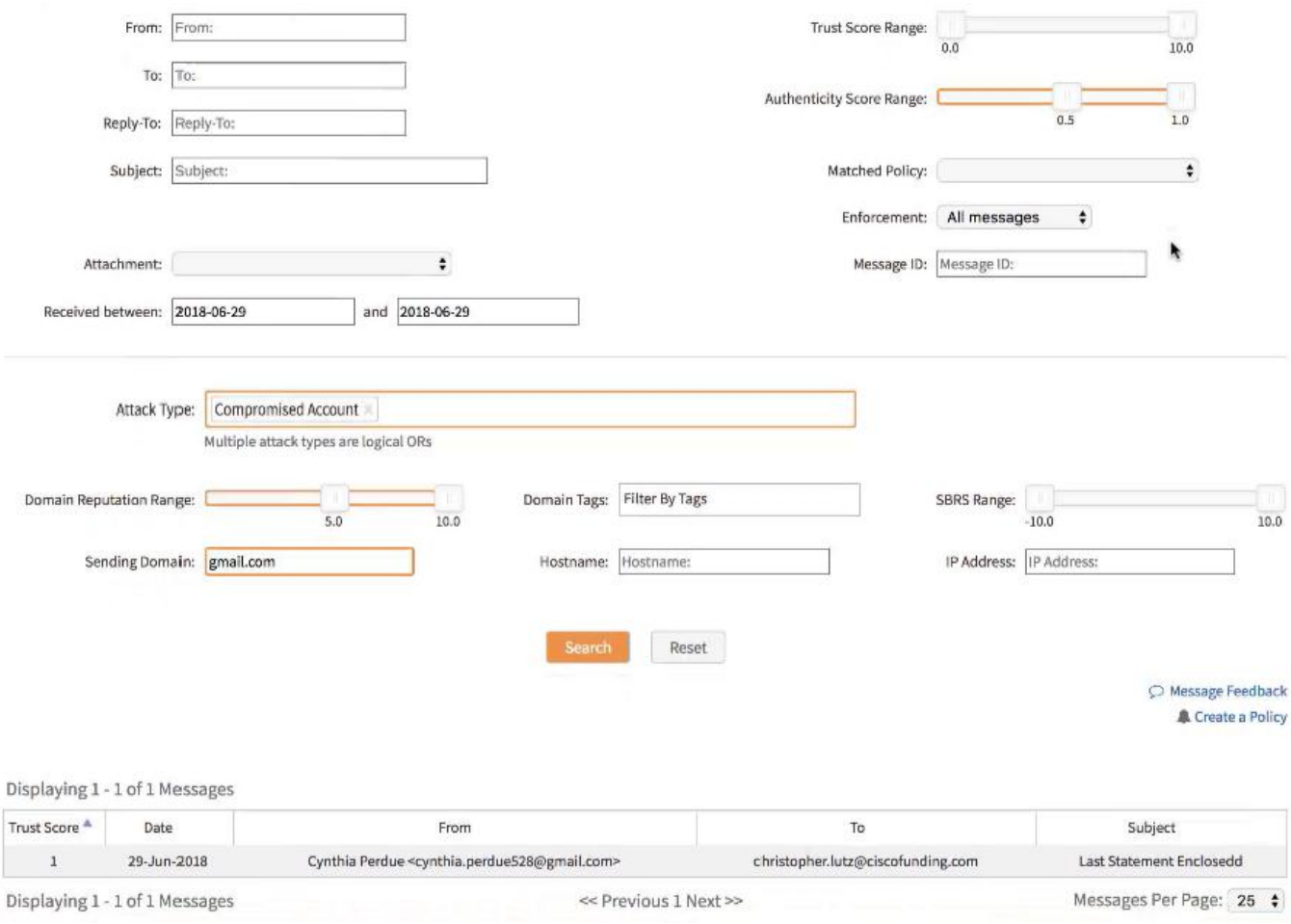
1. [侵害を受けたアカウント（Compromised Accounts）] をクリックします。

このメッセージは実際には信頼できる区画に表示されています。その理由は、侵害されたアカウントがスプーフィングではなく、必ずしもなりすましとは断定されないからです。これは、実在のユーザから盗まれた ID です。

2. [gmail.com] の円をクリックします。

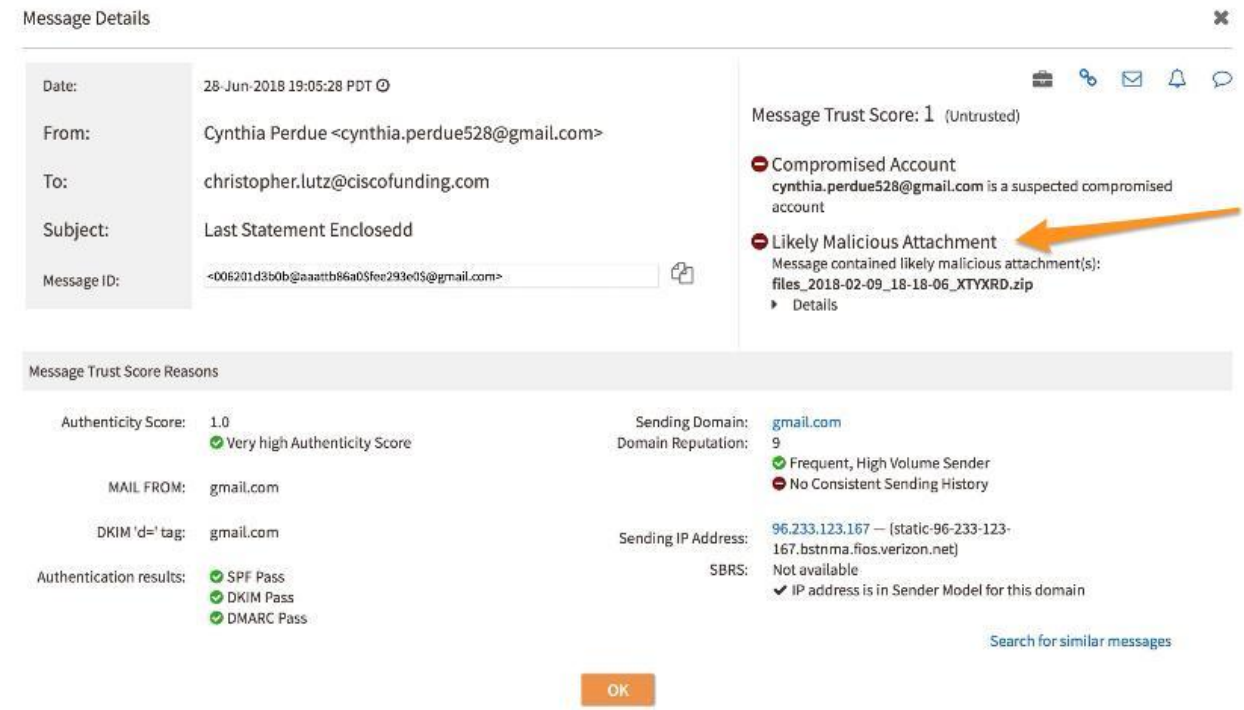


この例の場合、Cynthia Perdue というユーザの本物のアカウントであり、これまでは正当に使用されていたことが、シスコのモデルからわかります。

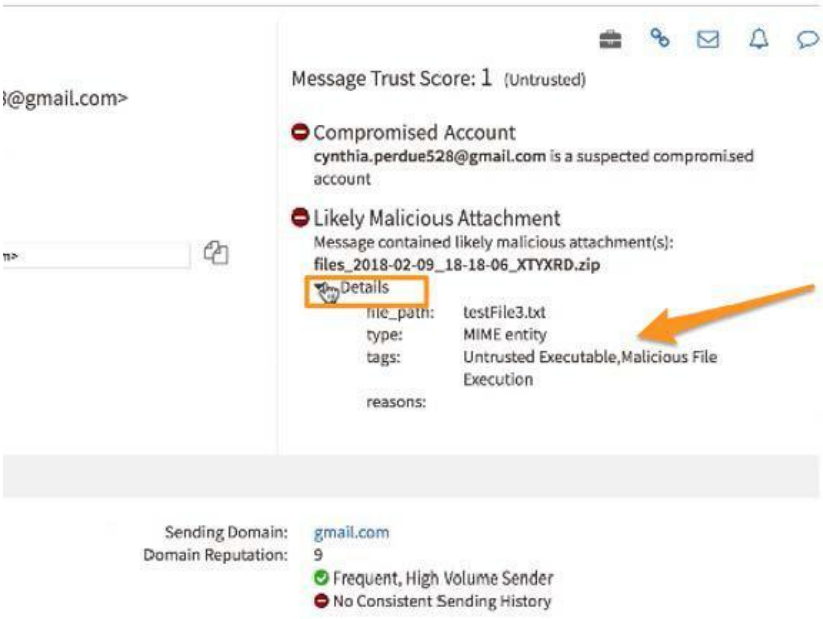


3. **メッセージ**をクリックします。

ここでは、信頼できない実行可能ファイルを含む添付ファイルを送信しているアカウントとして検出されています。このように、これまで良好だったアカウントから突然不正な動作が見られた場合、侵害の可能性が強いと言えます。



4. [詳細（Details）] をクリックします。



添付ファイルは、[悪意のあるファイルの実行（Malicious File Execution）] を伴う [信頼できない実行可能ファイル（Untrusted Executable）] と分類されています。

5. **シスコのロゴ**をクリックして [概要（Overview）] ページに戻ります。

シナリオ 4.　表示名偽装によるビジネス メール詐欺

ビジネス メール詐欺（BEC）は、多くの場合、表示名偽装を利用して実行されます。表示名偽装は、各社の役員や有名ブランドになりすますために犯罪者が使用する、一般的な手口です。Advanced Phishing Protection では、この両方の種類の攻撃を特定することができます。

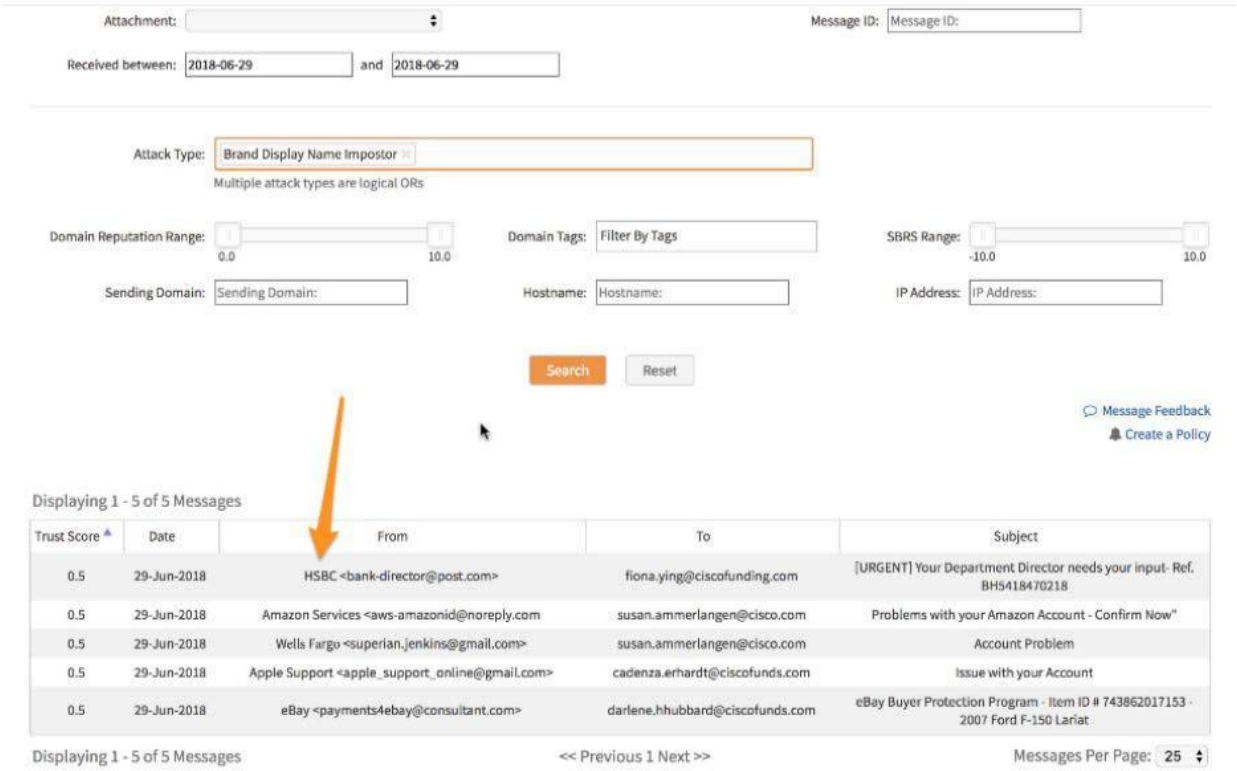
手順

1. [ブランド表示名なりすまし（Brand Display Name Imposters）] をクリックします。

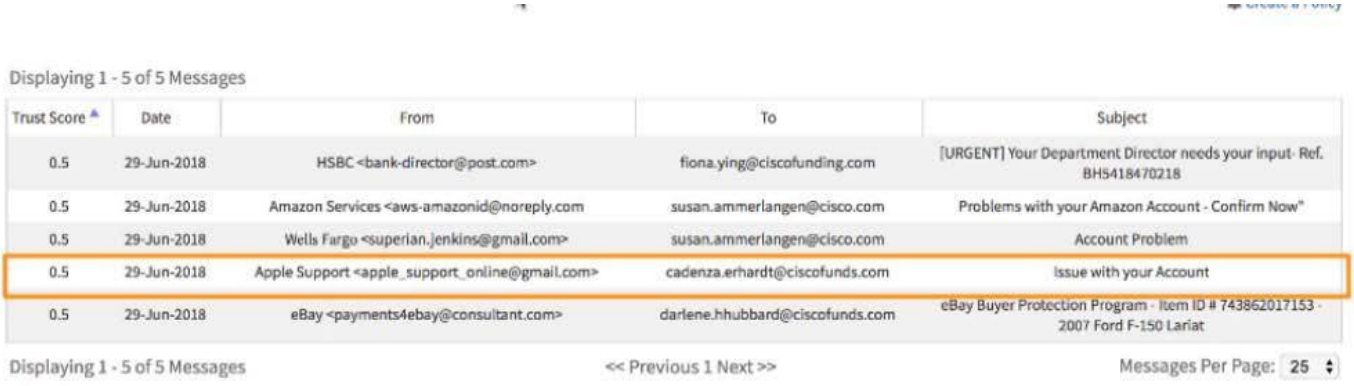
現在、5 件のブランド表示名なりすましが確認されています。ここでは、その送信元ドメインの簡単な概要を表示します。

2. [メッセージの表示（Show Messages）] をクリックします。

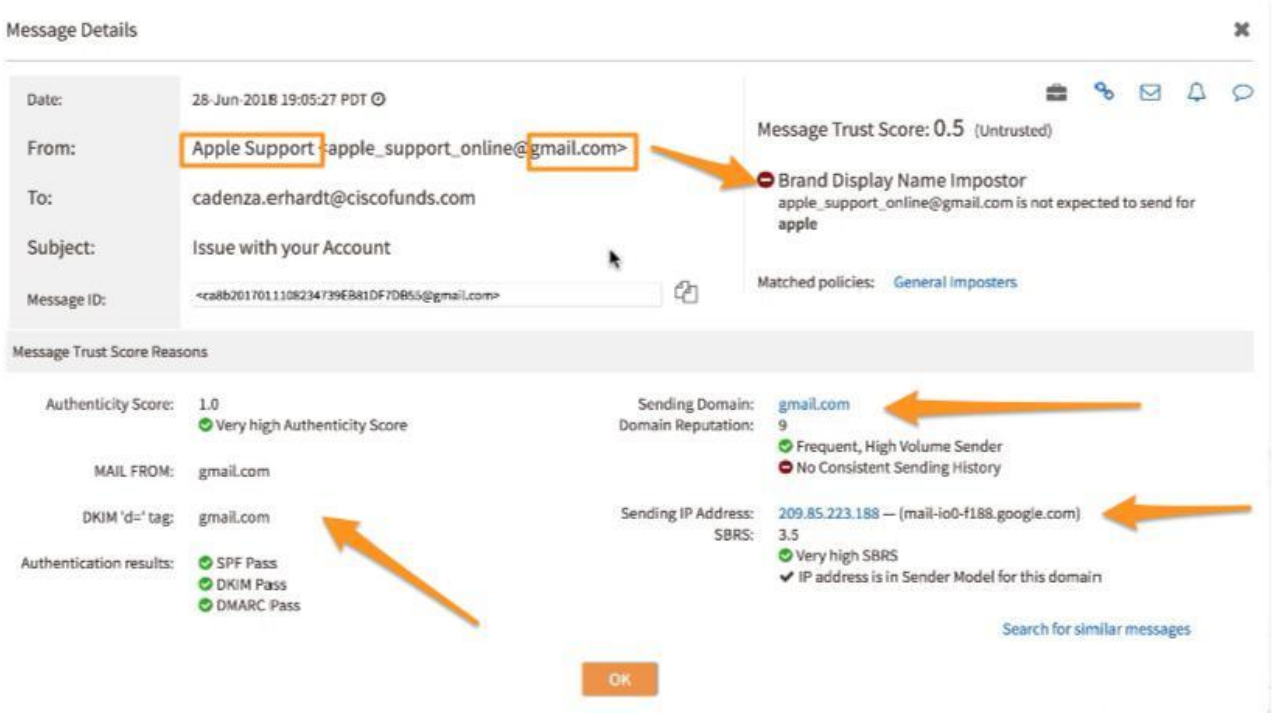
ここに表示されている HSMC、Amazon、Wells Fargo、Apple、eBay という大手ブランドはすべて、現在なりすましの対象になっています。



3. [Apple Support] のメッセージをクリックします。



このメッセージは、レピュテーションの高い送信者である Gmail から着信したものであり、Gmail のインフラストラクチャから正当に送信されていますが、Apple サポートが gmail.com アドレスのアカウントを使って受信者アカウントの問題を通知するとは、通常は考えられません。



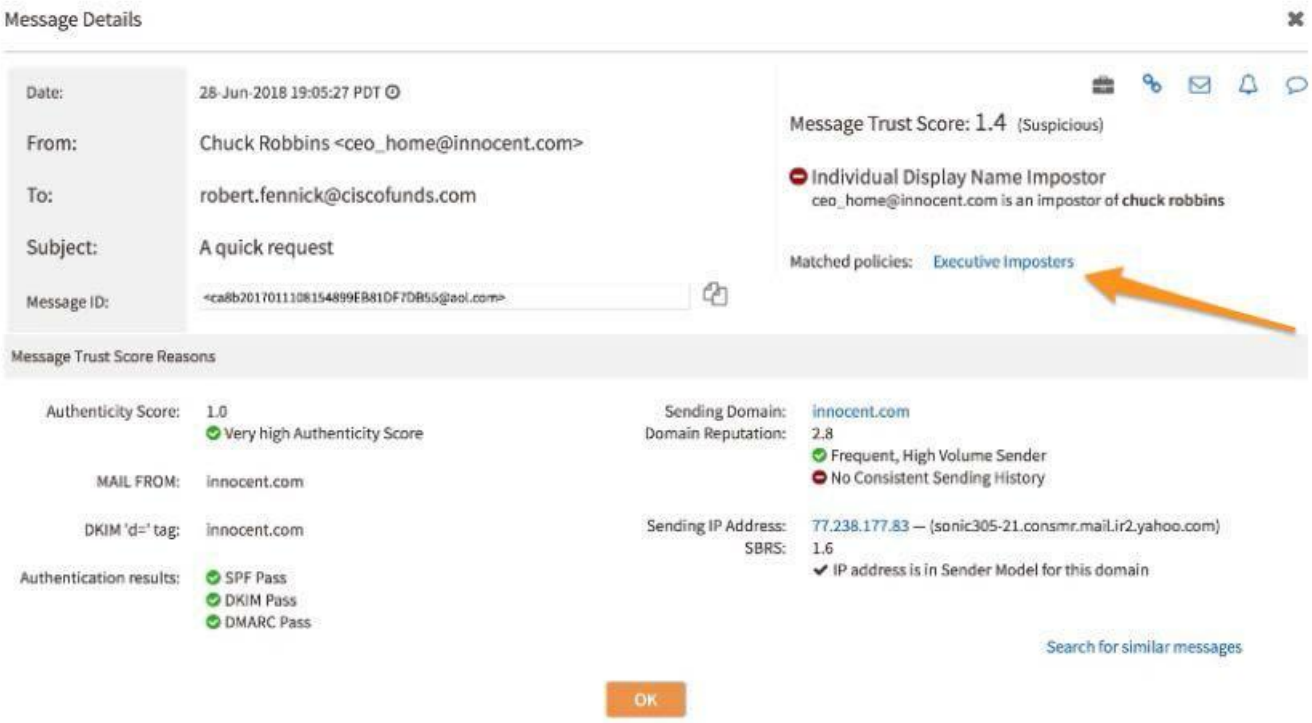
4. [OK] をクリックします。
5. **シスコのロゴ**をクリックして [概要（Overview）] ページに戻ります。
6. [個々の表示名なりすまし（Individual Display Name Imposters）] をクリックします。

7. [メッセージの表示（Show Messages）] をクリックします。

よくあるように、最高責任者がターゲットになっています。

8. **CEO** のメッセージ（Chuck Robbins へのなりすまし）をクリックします。

このなりすましメッセージの詳細を見るときは、[合致するポリシー（Matched policies）] に特に着目してください。この例でのポリシー名は、[役員のなりすまし（Executive Impostors）] です。



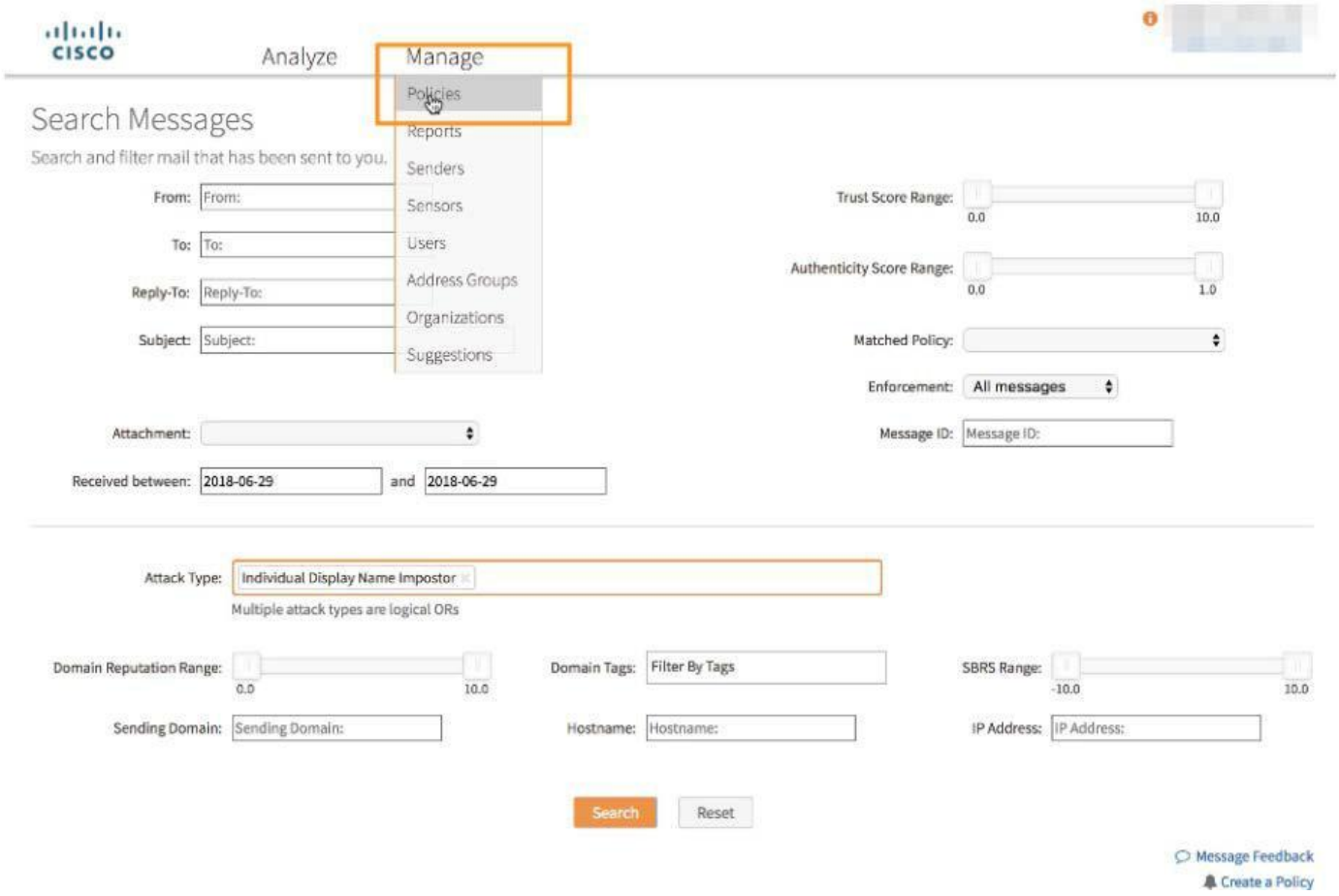
9. [OK] をクリックしてから**シスコ**のロゴをクリックして [概要（Overview）] ページに戻ります。

シナリオ 5.　ポリシー

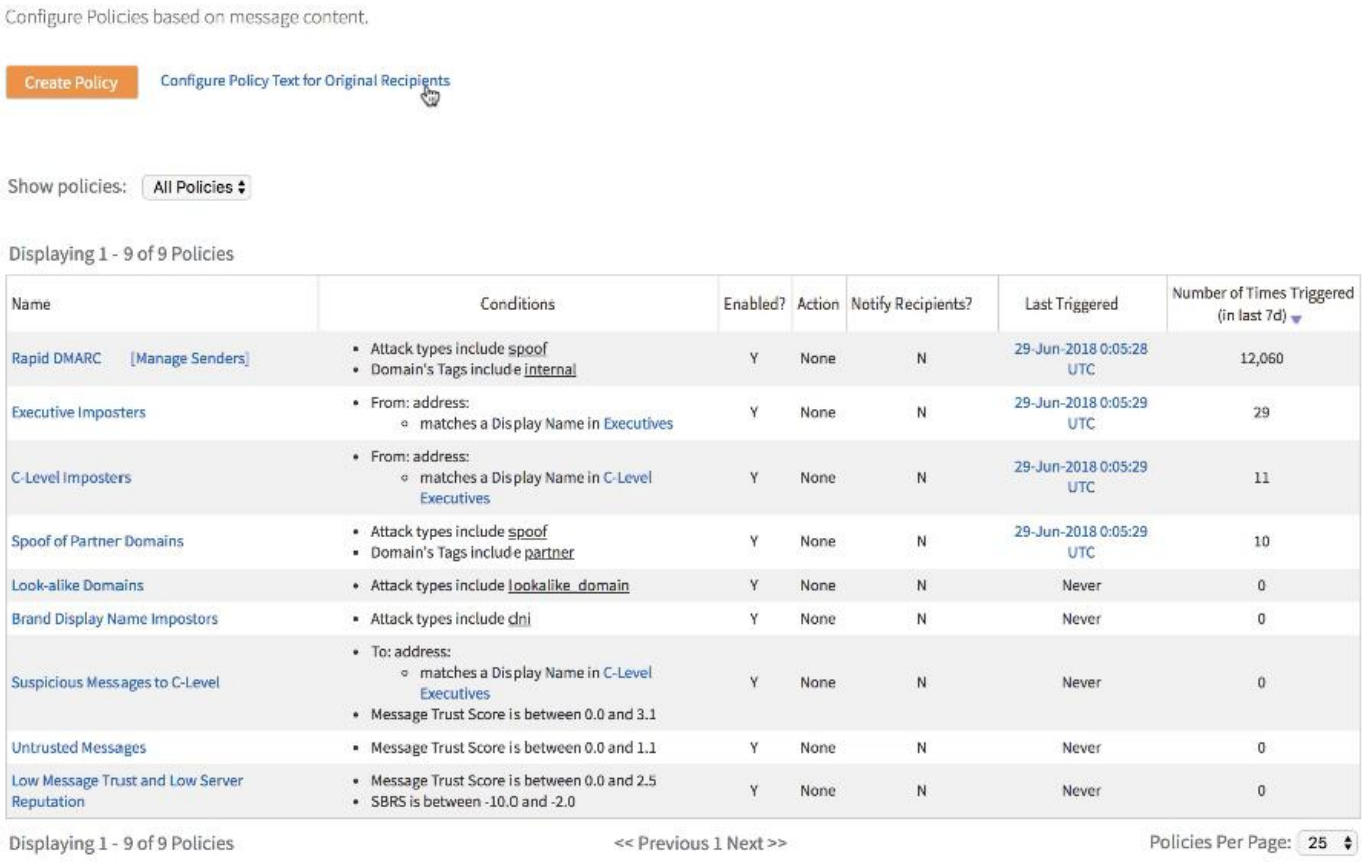
悪意のあるメッセージを識別するには、信頼スコアと攻撃の分類が使用されます。ポリシーとは、これらに基づいてどのようなアクションを行うか指定するルールです。使用可能なアクションの種類としては、セキュリティ管理者または SOC に対するアラート、メッセージの本来の受信者に対するアラート、メッセージの削除、受信トレイから別フォルダ（迷惑メールなど）へのメッセージの移動などの機能があります。

手順

1. [管理（Manage）] > [ポリシー（Policies）] の順に移動します。

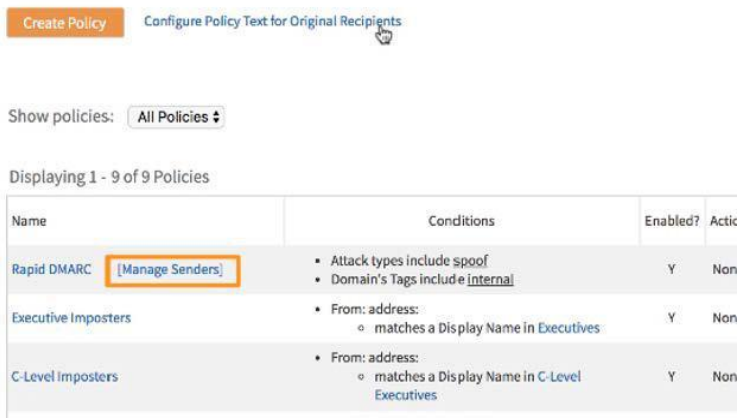


下記に示しているのは、メッセージの信頼スコアと攻撃の種類を使用した、最も一般的な攻撃の条件をカバーするデフォルト ポリシー セットです。

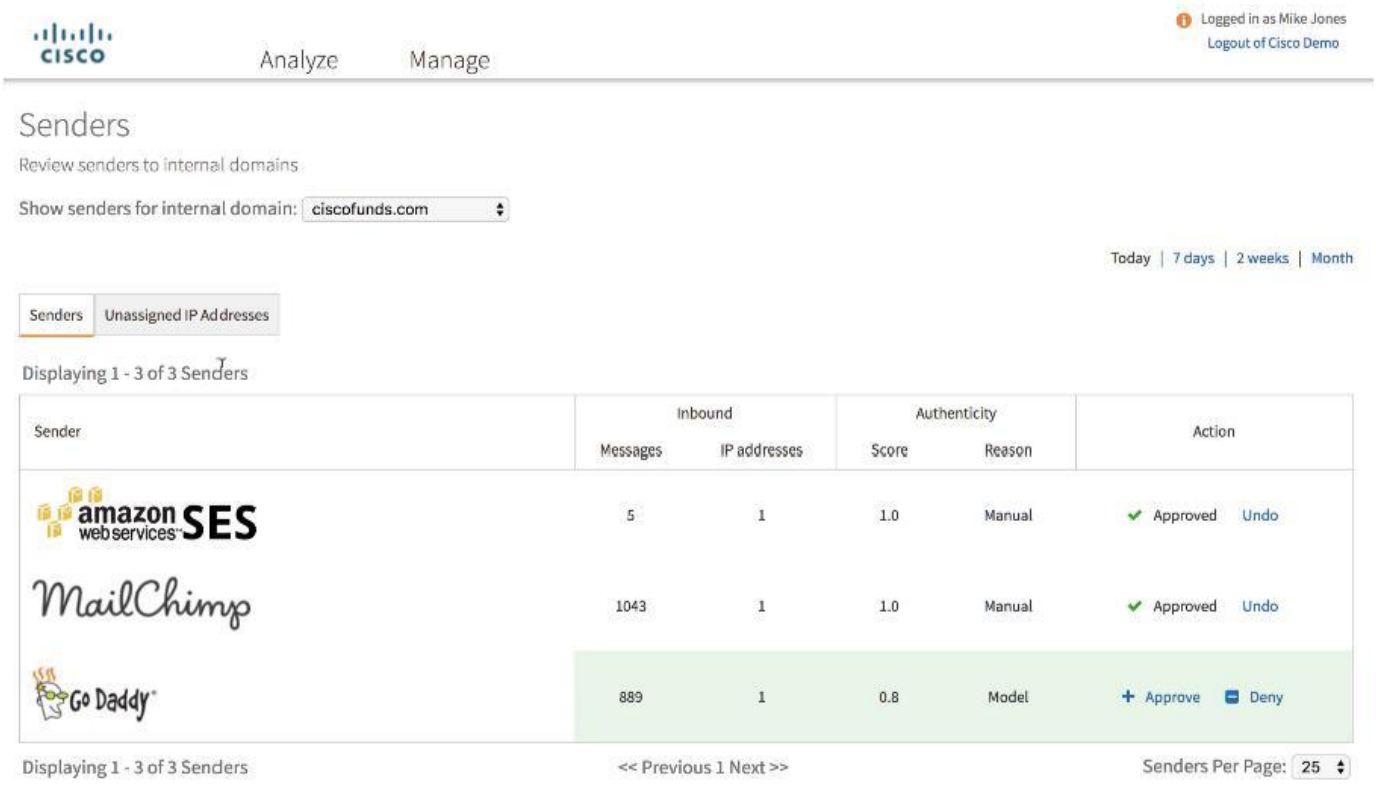


Rapid DMARC ポリシーは、パブリック DMARC 拒否ポリシーを発行するよりも短時間のうちに、自ドメインを着信スプーフィングから保護できる、特別なポリシーです。ポリシー条件が社内ドメインのスプーフィングを特定する設定になっていることに注目してください。ポリシーの横にある [送信者の管理（Manage Senders）] リンクをクリックすると、Advanced Phishing Protection の信頼モデルをガイドとして使用し、すべての送信者をすばやく簡単にカタログ化することができます。送信者のカタログ化を行わない場合でも、ポリシーはデフォルトで、Advanced Phishing Protection 信頼モデルを使用して機能します。

2. ポリシー名 **Rapid DMARC** の横にある [送信者の管理（Manage Senders）] リンクをクリックします。

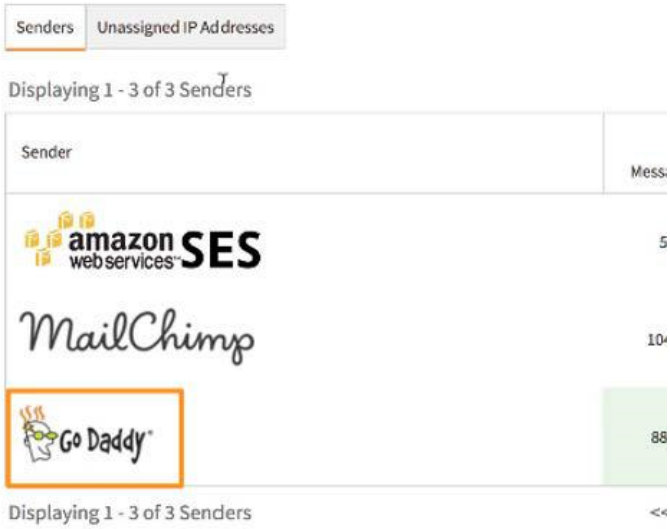


これらは、シスコの社内ドメイン ciscofunds.com に対する送信者です。

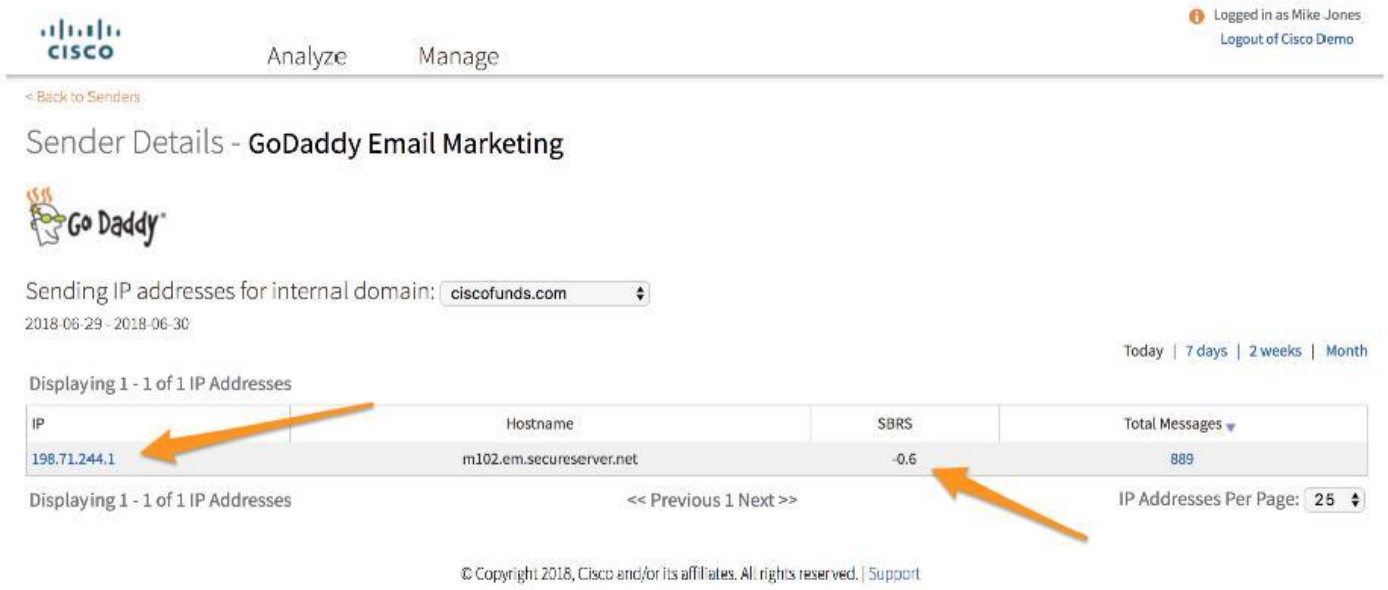


この例では、Amazon SES および Mail Chimp の 2 つの送信者が [承認済み（Approved）] となっています。つまり、これらはすでに、このドメイン向けの正当な送信者としてカタログ化されています。もう 1 つの送信者、GoDaddy については、信頼できるものとしてモデリングされていますが、カタログには追加されていません。これを追加すべきでしょうか。判断するには、詳細を確認する必要があります。

3. **GoDaddy** のロゴをクリックします。

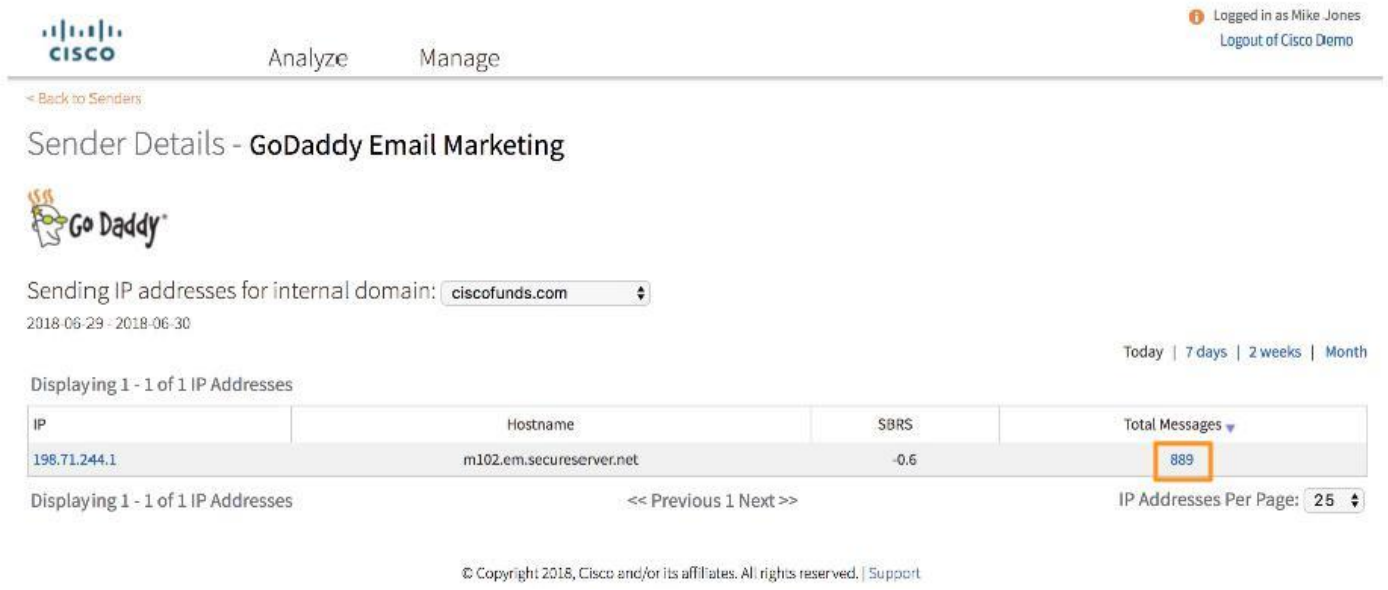


メッセージはすべて、下記に示す GoDaddy の 1 つのサーバから発信されています。



このサーバの SenderBase レピュテーション スコア（SBRS）は、あまり良好ではありません。メッセージ数をクリックすると、より詳しい情報を確認できます。

4. **メッセージ数**をクリックします。



クリックすると、その一連のメッセージが示された [メッセージの検索（Search Messages）] ページが表示されます。リストを調べて、認識している送信者かどうか確認できます。件名または送信元詳細をコンテキスト上の手がかりとして、信頼できるメッセージかどうかを確認できます。インベントリに追加したい送信者であることが確認できた場合は承認し、そうでない場合では拒否することができます。

5. ブラウザの [戻る（Back）] ボタンを 2 回をクリックして [送信者（Senders）] ページに戻ります。
6. **送信者**を承認または拒否します。
    - 正当な送信者と思われる場合は、GoDaddy の [承認（Approve）] リンクをクリックします。

    - 正当ではないと思われる場合は、GoDaddy の [拒否（Deny）] リンクをクリックします。

7. どちらの場合も、**選択を確定**します。

ここで選択したオプションによって、今後この送信者から ciscofunds.com 宛てにメッセージが送信された場合に、正当と見なされるのかスプーフィングと見なされるのかが左右されます。

8. **シスコのロゴ**をクリックして [概要（Overview）] ページに戻ります。

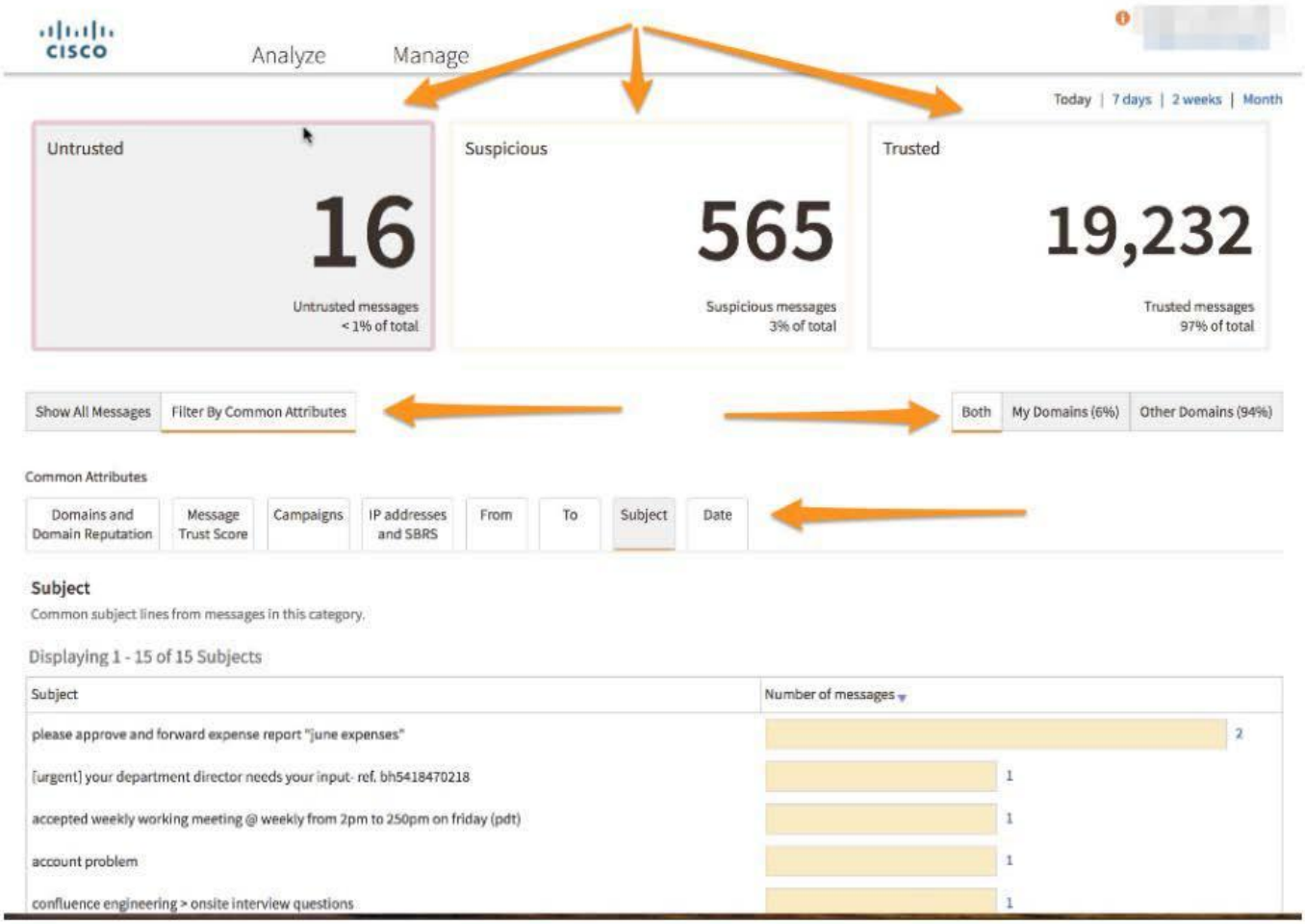
シナリオ 6.　メッセージの分析

Advanced Phishing Protection では、電子メール トラフィックについて把握するための分析ビューが数多く提供されています。信頼できないメッセージ、疑わしいメッセージ、信頼できるメッセージの概観をつかむ方法として、[メッセージ（Messages）] ビューが一般的に利用されています。

手順

1. [分析（Analyze）] > [メッセージ（Messages）] の順に移動します。

これらの信頼性範囲それぞれについて、さまざまな一般的属性に基づくビューのフィルタリングを選択し、分析することができます。



2. [一般的属性でフィルタリング（Filter By Common Attributes）] をクリックしてから [件名（Subject）] をクリックし、続いて [疑わしいメッセージ（Suspicious）] をクリックします。

3. **シスコのロゴ**をクリックして [概要（Overview）] ページに戻ります。

本書は Cisco Advanced Phishing Protection の機能についての簡単なデモ資料ですが、皆様にとって有益なものとなることを願っています。Cisco Advanced Phishing Protection を利用すれば、現在最も複雑な BEC および ATO 攻撃で使用されている ID 偽装手法をも阻止することが可能です。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp