ドキュメント タイプ

デモンストレーション ガイド

Cisco Email Security Threat Analyzer v3

Cisco E メール セキュリティのテクニカル マーケティング エンジニアと共同作成。

最終更新日：2020 年 6 月 20 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

制約

Office 365 向け Cisco E メール セキュリティ Threat Analyzer ツールには以下の制約があります。

- [すべてのメールボックス（All Mailboxes）]オプションは、デフォルトで 50 個のメールボックスをスキャンします。スキャンするメールボックスの数は変更できます。
- スキャンは、メールボックスあたり 2,500 通のメールに制限されます。
- すべてのスキャン オプションは、999 個のメールボックスに制限されます。

要件

次の表に、このデモンストレーションの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	Cisco AnyConnect®

このソリューションについて

多くのお客様が、電子メール戦略の一環として従来のオンプレミスの Microsoft Exchange からクラウドベースの Office 365 に移行しています。それに伴い、電子メールに対するより強力なセキュリティ ソリューションの必要性が増しています。

このデモンストレーションでは、無料で使用できる、システムに影響を与えない Cisco Office 365 Threat Analyzer の利点を紹介します。Cisco E メール セキュリティに統合されたこのツールは、アプリケーション プログラミング インターフェイス（API）を利用して特定された Microsoft Office 365 のメールボックスをスキャンします。そして、Microsoft Office 365 電子メール環境に潜むスパム、ウイルス、グレイメール、マルウェアなどの脅威に関する有益な情報をレポートします。

注：このツールを使用して、レポートによって特定されたメッセージまたは脅威を修正できるわけではありません。

Cisco E メール セキュリティは、送受信メールに対する優れたクレンジング機能と制御機能を備えています。今日の電子メールに絶え間なく影響を与える、動的で変化の速い脅威に対し、お客様のニーズに合ったさまざまなフォーム ファクタで可用性の高い電子メール保護を実現します。

Cisco クラウド E メール セキュリティの詳細については、http://www.cisco.com/web/JP/product/hs/security/emailsecurity/Products_Sub_Category_Home.html を参照してください。Cisco E メール セキュリティの機能と利点、利用可能なフォーム ファクタ、シスコの差別化要因などの詳細をご覧いただけます。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント クレデンシャルは、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックするか、それらを使用するシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

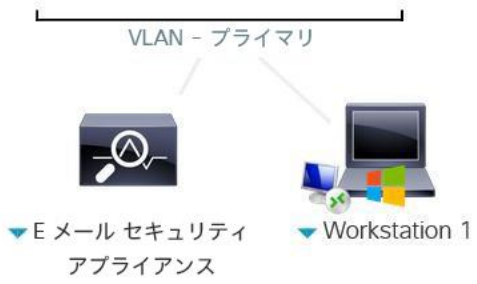


図 2. 物理トポロジ

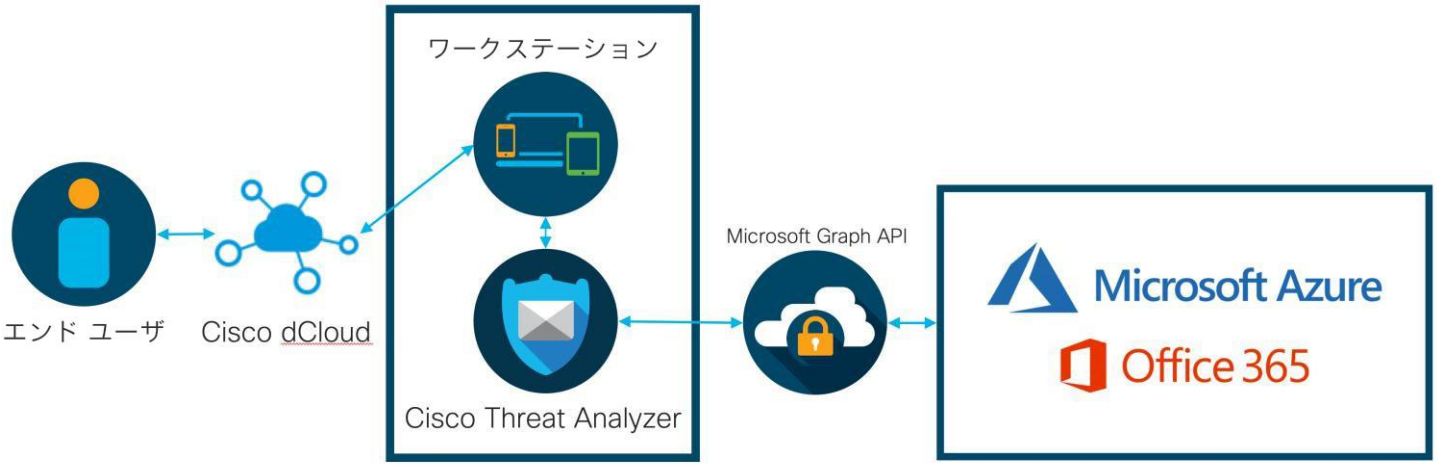


表 2. 機器の詳細

名前	説明	ホスト名（FQDN）	IP アドレス	ユーザ名	パスワード
電子メール セキュリティ アプライアンス	O365 向け Threat Analyzer ツールを実行する	esa.dcloud.cisco.com	198.18.133.146	admin	C1sco12345
ワークステーション 1	Cisco E メール セキュリティ アプライアンス TA へのアクセスに使用される Windows 7 ワークステーション	wkst1.dcloud.cisco.com	198.18.133.36	administrator	C1sco12345

ドキュメント タイプ

デモンストレーション ガイド

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には入念な準備が不可欠です。

O365 向け Cisco E メール セキュリティ Threat Analyzer ツールのスケジュール設定

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. dCloud セッションを開始します。[**手順を見る**] [英語]

注：セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るために、Cisco AnyConnect VPN [**手順を見る**] およびラップトップのローカル RDP クライアント [**手順を見る**] を使用してワークステーションに接続します。

ワークステーション 1：**198.18.133.36**、ユーザ名：**administrator**、パスワード：**C1sco12345**

注：Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [手順を見る] [英語]。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法では、接続ができない場合や、パフォーマンスが悪い場合があります。

重要：Threat Analyzer ツールは事前設定済みです。vESA 内で、関連するスキャン エンジンの設定値を管理または変更する必要はありません。vESA を直接管理すると、想定外のレポートまたはエラーの原因となる可能性があります。

設定の変更が必要な場合、パートナーはオンプレミスのインスタンスを起動して使用することをリクエストできます。詳細についてはオンプレミスの O365 向け Threat Analyzer ページを参照してください。

注：シナリオ 1 のすべてのアクションは、お客様が自身の環境内で実行する必要があります。

スキャンを開始する前に、お客様は O365 向け Cisco Threat Analyzer を Microsoft Azure 環境に登録し、必要な権限を付与する必要があります。これを完了した後、お客様はクライアント ID/アプリケーション ID およびテナント ID を提示する必要があります。この情報がないと、Cisco dCloud 環境内の API を登録できません。

ドキュメント タイプ

デモンストレーション ガイド

シナリオ 1： Microsoft Azure アプリケーションの作成

価値提案：Microsoft Azure はサービスとしてのプラットフォーム（PaaS）ソリューションで、Microsoft の製品を使用し、Microsoft のデータセンターにソリューションを構築およびホスティングできます。包括的なクラウド製品のスイートで、ユーザは独自のインフラストラクチャを構築しなくても、容易にエンタープライズ規模のアプリケーションを作成できます。

セキュリティのために、Threat Analyzer との連動は読み取りのみとなっています。ユーザの ID とクレデンシャルを管理でき、さらにアクセスを制御できるため、ビジネスと個人の情報を保護できます。

Threat Analyzer ツールを実行する前に、Microsoft Azure から Threat Analyzer への API 接続を作成する必要があります。この情報はお客様側が提供します。API を開いて必要なクライアント ID とアプリケーション ID を提示するための一連の手順を、お客様が確認できるように、シナリオ 1 をコピーしてお客様に提供できます。

前提条件

- Office 365 アカウントのサブスクリプション。Enterprise E3 または Enterprise E5 アカウントなど、Microsoft Office 365 アカウントのサブスクリプションに Exchange が含まれていることを確認してください。
- Microsoft Azure 管理者アカウントと http://portal.azure.com へのアクセス
- Microsoft Office 365 と Microsoft Azure AD アカウントの両方がアクティブな *user@domain.com* 電子メールアドレスに適切に結び付けられ、このドメインおよびアカウントから電子メールを送受信できる必要があります。

アプリケーションの登録

1. Microsoft Azure ポータル（https://portal.azure.com）にログインします。
2. [Azure Active Directory] をクリックします。
3. [アプリケーションの登録（App registrations）] をクリックします。
4. [新しいアプリケーションの登録（New application registration）] をクリックし、以下の必須フィールドに入力します。
   - [名前（Name）]：**Threat Analyzer**（または任意の名前）
   - [アプリケーション タイプ（Application type）]：[Web アプリ/API（Web app / API）]
   - [サインオン URL（Sign-on URL）]：https://www.cisco.com/sign-on
5. [作成（Create）] をクリックします。
6. [設定（Settings）] をクリックします。
7. [必要な権限（Required permissions）] をクリックします。

b. [+ 追加（+Add）] をクリックします。

c. [API の選択（Select an API）] をクリックし、API のリストから [Microsoft Graph] を選択します。

d. 一番下で [選択（Select）] をクリックします。

e. [アプリケーション権限（Application Permissions）] に以下の権限を選択します。

- [すべてのグループの読み取り（Read all groups）]
- [ディレクトリ データの読み取り（Read directory data）]
- [すべてのメールボックスのメールの読み取り（Read mail in all mailboxes）]

f. 下にスクロールし、同様に、[代理権限（Delegated Permissions）] に以下の権限を選択します。

- [ユーザ メールを読み取り（Read user mail）]
- [すべてのグループの読み取り（Read all groups）]
- [ディレクトリ データの読み取り（Read directory data）]

g. 一番下で [選択（Select）] をクリックします。

h. [完了（Done）] をクリックします。

i. 最後に [権限の付与（Grant permissions）] をクリックして、新しい権限をアプリケーションに適用します。

注意：権限の付与

上記の手順を完了した後に権限の付与を適用**しない**場合、アプリケーションは Threat Analyzer ツールに接続できず、API エラーが表示されます。

マニフェストの編集

注：自分のラップトップからコピーして WKST1 に貼り付ける場合は、必要になるまで、Notepad などのテキスト エディタを使用してデータを保存しておきます。WKST1 内の Azure ポータルを開いて設定した場合は、<Ctrl>+<Alt>+<Shift> を使用してデータおよび/または ID をコピーして貼り付けます。Apple Mac ユーザの場合、ローカル マシンから dCloud のワークステーションにコピーするためのキーの組み合わせは <CTRL>+<OPTION>+<SHIFT> です。これによってリモート デスクトップ クリップボードが表示され、データを交換できます。

1. メインの登録アプリケーション ペインから、[マニフェスト（Manifest）] をクリックします。
2. 以下を**そのまま**コピーして、**keyCredentials** 行を置き換えます。

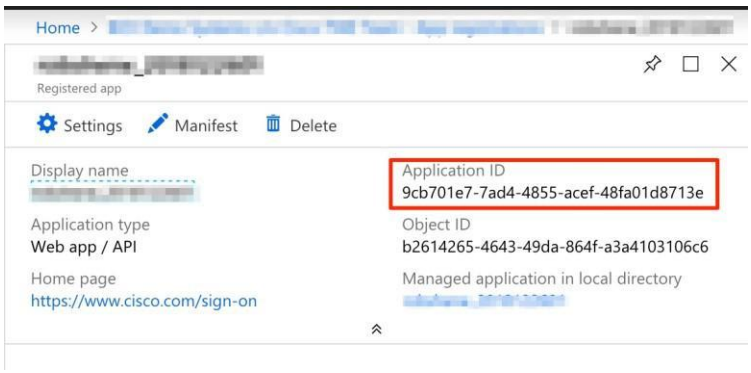
```
"keyCredentials": [{
"customKeyIdentifier": "B2ybFYpimVk+etGYPZX9QvIAgw8=",
"keyId": "169acc09-1d17-4235-8eb1-22a387b494c4",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value":
"MIIDiTCCAnGgAwIBAgIBATANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExCzAJBgNVBAcTAkNBMQ4wDAYDVQQ
KEwVDaXNjbzEMMAoGA1UECxMDRVNBMQwwCgYDVQQDEwNFU0ExIDAeBgkqhkiG9w0BCQEWEWVzYS10bWVAY2lzY28uY29tMB4XDTE3MDcxODA
wMDAwMFoXDTI3MDcxNzIzNTk1OVowdTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQswCQYDVQQHEwJDQTEOMAwGA1UEChMFQ2lzY28xDDA
KBgNVBAsTA0VTQTEMMAoGA1UEAxMDRVNBMSAwHgYJKoZIhvcNAQkBFhFlc2EtdG1lQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggE
PADCCAQoCggEBAKEpwf9e/Fyh2tc4r+9+J59SXOKwWx9ODu7K5P7I2KTa2QwPyahp+ehvOGvbknAnwhnJ+d1mwy5NsoQ9MQtcAmrZQXaeqJG
mf2Nke/AwQXkth8uDrIWo9D5FCuU35W0+C4Hv2Gn1BBt38mvItReaye5Iqe8Nr2shI8k8kCYa3Gk5jWnp02LllcRETo9/CwWAfhaE6T9XlAR
XevB6M9Y6Ua0zu2sM4MIdeR74+1D3ZIK57yElGubuymZ7AsrYWVrQ1iM5rJpemS/kNsSrULsZl4PX63/eRw9lvY1HK9+yOYdI6J4aSaQl8jR
h1hEHdzZowPq82dCsNptGEaCUsGZuYdcCAwEAAaMkMCIwCwYDVR0PBAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA0GCSqGSIb3DQEBBQU
AA4IBAQAK6H5v3mq+ng1gqnQ3pX+K6PjMTYrDTKrkM+6slaV1jv9TRHfM5xrQjInkO+evQrCnnn/Pg6AhkfYbivFsMZiN0yTUind9lNgIOx/
ZJqcsnZrr3M8Y8xLa7zrM6sxV5fNzpun2Ly0fKHN90eNpTyixp31rgINLCmsm9w9UqV5+VVkubt0c9fS2BQOSsJzR613kfvCPjI4h7ppYypc
ERnNgXxlJrJGcu4F6Hzsf2QJVhlYgKN8+VoBhtlmlX7EqaoTloH53f7/b4lB2pG9DT7raE9IkGJ3Hw2AtoQQwLIjYivYKwd6JO3+pO3w2KzD
pJ7GQPNW6UzN4waITfDMevcRz"
}],
```

注：MIIDiTCC から始まり DMevcRz で終わる値の文字列は、1 行にする必要があります。文字列の編集には Notepad テキスト エディタを使用することをお勧めします。

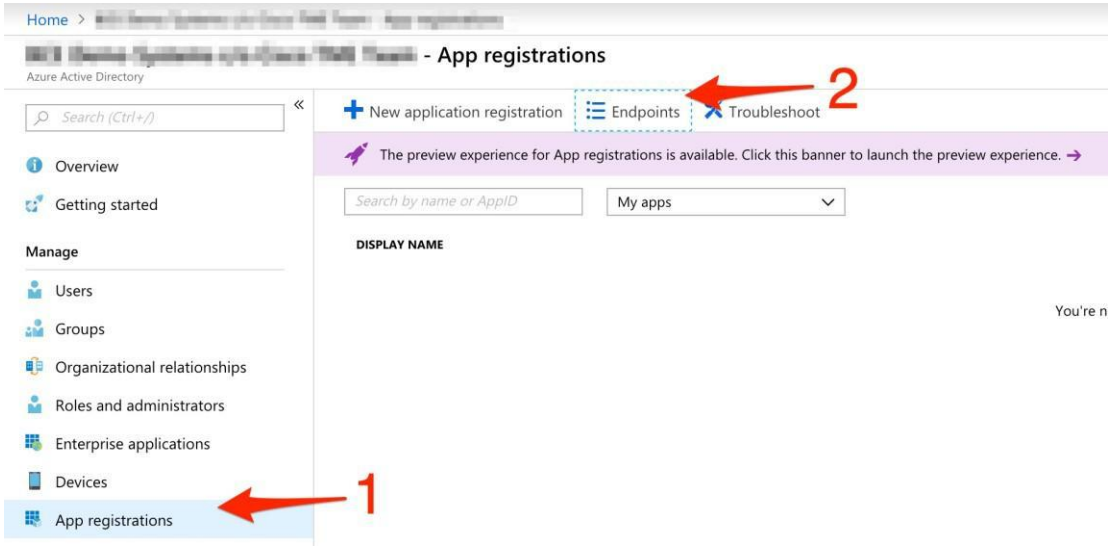
3. [マニフェストの編集（Edit Manifest）] ペインで [保存（Save）] をクリックします。

クライアント ID とテナント ID の取得

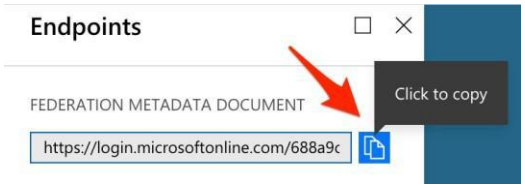
1. Azure ポータルのクライアント ID は [アプリケーション ID（Application ID）] という名前です。これは、作成したアプリケーションのメイン ペインで見つけることができます。



2. テナント ID は、最初のレベルの [アプリケーションの登録（App Registrations）]>[エンドポイント（Endpoints）]ペインで見つけることができます。



- **テナント ID** はこの文字列内のあります。右側で、列挙されるいずれかの文字列をコピーします。



例：

```
...windows.net/688a9cde-c495-44d8-afb2-ae1234567890/federationmetadata/2007-06/federationmetadata.xml
```

この例では、テナント ID は **688a9cde-c495-44d8-afb2-ae1234567890** です。

注：これは 16 進数の形式で、表記は 8:4:4:4:12 となります。

例：1234abcd-12ab-34cd-12ab-123456789abcd

このドキュメントの例では、最終的な ID は以下の通りです。

- クライアント ID = アプリケーション ID： 9cb701e7-7ad4-4855-acef-48fa01d8713e
- テナント ID： 688a9cde-c495-44d8-afb2-ae1234567890

Azure アプリケーションの作成の完了

この時点で、以下の情報を作成しました。

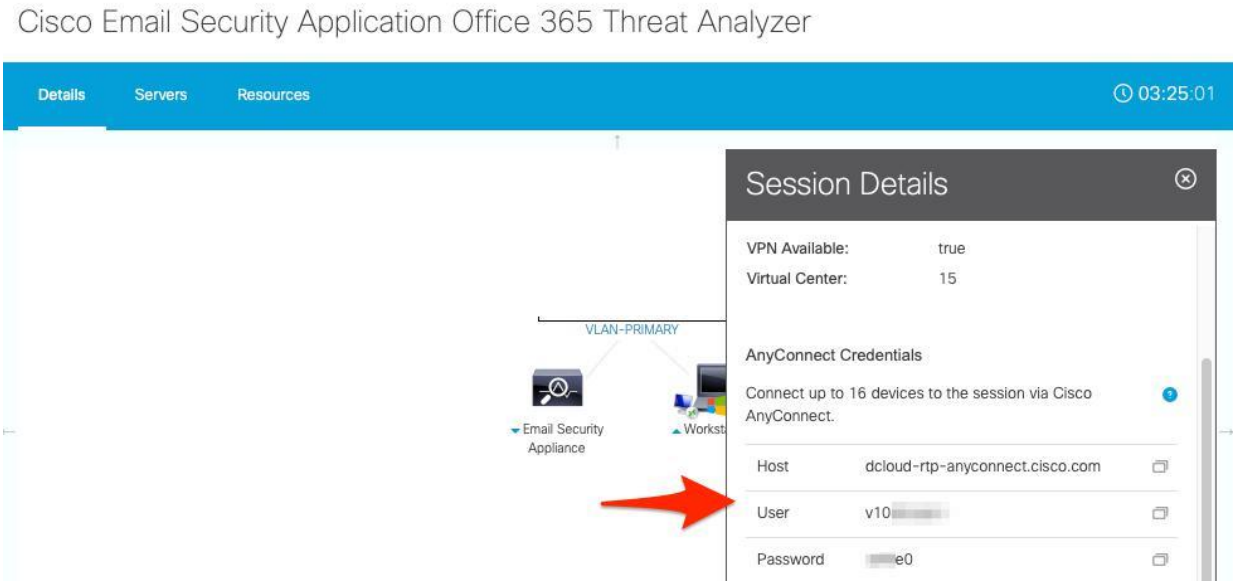
- クライアント ID（またはアプリケーション ID）
- テナント ID

これで、Threat Analyzer ツールを開始する準備が整いました。

シナリオ 2： O365 向け Cisco Threat Analyzer の起動

価値提案：O365 向け Cisco Threat Analyzer ツールは、リモート デスクトップを使用するか、Cisco AnyConnect によって Cisco VPN サーバへの仮想プライベート ネットワーク（VPN）を確立することで、Cisco dCloud 環境から直接実行できます。[手順を見る]

以下の手順では、dCloud ワークステーションとリモート デスクトップのオプションを使用することを想定しています。VPN 経由でのアクセスについては、Cisco dCloud セッションの [情報（Info）] または [セッションの詳細（Session Details）] セクションに記載された詳細を参照してください。



O365 向け Cisco Threat Analyzer の開始

1. 「はじめに」セクションの手順を使用して、dCloud の **Workstation 1** に接続します。
2. デスクトップで、**Cisco Threat Analyzer** のショートカットを開きます。
3. Google Chrome が起動され、ランディング ページとして *ReadMe* ドキュメントがロードされます。
4. ツールを起動するには、**Cisco Threat Analyzer** のブックマークをクリックします。
5. 以下のアクセス クレデンシャルでログインします。
   - ユーザ名：**admin**
   - パスワード：**C1sco12345**
6. 以下の情報を入力します。
   - [顧客名（Customer Name）]：**自分の会社名**（Outdoor Sports, Inc など）
   - [クライアント ID（Client ID）]：(シナリオ 1 で取得)
   - [テナント ID（Tenant ID）]：(シナリオ 1 で取得)
   - [サムプリント（Thumbprint）]：B2ybFYpimVk+etGYPZX9QvIAgw8=（注を参照）

注：自分のラップトップからコピーして WKST1 に貼り付ける場合は、必要になるまで、Notepad などのテキスト エディタを使用して ID を保存しておきます。WKST1 内の Azure ポータルを開いて設定した場合は、<Ctrl>+<Alt>+<Shift> を使用して ID をコピーして貼り付けます。Apple Mac ユーザの場合、ローカル マシンから dCloud のワークステーションにコピーするためのキーの組み合わせは <CTRL>+<OPTION>+<SHIFT> です。これによってリモート デスクトップ クリップボードが表示され、データを交換できます。

注：または、サムプリントはデスクトップの「Client and Tenant IDs.rtf」というファイルから直接コピーすることもできます。

7. [証明書秘密鍵（Certificate Private Key）] を設定するために、[参照（Browse）] をクリックします。
   - [ファイルのアップロード（File Upload）] ウィンドウで、C:\Users\Administrator\Downloads\Supporting Info フォルダから demo.pem を選択します。

注：自己署名証明書と秘密鍵は、スキャン タスクの効率化のために事前に定義されています。これらを使用することについてお客様に懸念がある場合、オンプレミスの場合の手順を使用して、必要な証明書、keyCredentials、サムプリントを生成できます。**「証明書：UNIX/Linux（openssh を使用）」および「証明書：Windows（Windows PowerShell を使用）」**を参照してください。パートナーは、オンプレミスのインスタンスを起動して使用することをリクエストすることもできます。詳細については、**オンプレミスの O365 向け Threat Analyzer ページ**を参照してください。

8. [検証（Validate）] をクリックします。API が検証されている間、簡単な確認メッセージが表示されます。
9. 検証が完了すると、以下のいずれかを選択してスキャンを開始できます。
   - LDAP グループ（LDAP Groups）
   - 次のメールボックス（Following Mailboxes）
   - 次のメールボックスを除外（Following Mailboxes are not）
   - すべてのメールボックス（All Mailboxes）

(*) スキャン前にお客様と話し、スキャンにどのメールボックスを含めるか、あるいは除外するかを特定しておいてください。スキャンによって電子メールと添付ファイルが概観されます。O365 向け Cisco Threat Analyzer ツールによるスキャンはすべてを包括したスキャンではなく、特定のメールボックスの受信箱における脅威とメール メッセージの簡単な確認のみを意図しています。

10. [スキャンの開始（Start Scan）] をクリックします。

注：[スキャンの開始（Start Scan）] ボタンをクリックしてから、API 経由でメールボックスが取得されるまでに少し時間がかかります。メールボックスが取得されるとダッシュボードが表示され、スキャンが実行されて進行中であることが分かります。

[例：Cisco Threat Analyzer ダッシュボード]

ダッシュボードを監視して更新とアクティビティを確認してください。ダッシュボード上部には、メールボックスのスキャン進行状況の割合、スキャン済みのメールボックスの数、スキップされたメールボックスの数が表示されます。スキップ済みのメールボックスの横に [#] がある場合は、[#] をクリックするとメールボックスがスキャンされなかった理由を確認できます。

何らかの理由でスキャンを停止する場合は、[スキャンの停止（Stop Scan）] をクリックし、ダッシュボードが更新されるのを待ちます。

シナリオ 3： Threat Analyzer レポートの生成

価値提案：Office 365 の受信トレイで検出されなかった脅威を可視化します。Office 365 のメールボックスに存在するセキュリティの脆弱性を特定します。また、Office 365 の電子メールに悪意のある URL、マルウェア、スパムがあるかどうかを判断します。

1. スキャンが完了したら、[エクスポート（Export）] をクリックしてお客様向けの PDF を生成します。
2. **emailScanReport.pdf** という名前の PDF が生成され、C:\Users\Administrator\Downloads に保存されます。
3. [Box – Cisco Log in] のブックマークを使用して Box にログインし、レポートを Box アカウントにアップロードします。

[例：Office 365 向け Cisco Threat Analyzer レポート]

4. レポートの結果は、vESA 自体から一覧化されます。dCloud セッションが引き続きスケジュールされていて利用可能な間に、Google Chrome ブラウザの [Cisco vESA] ブックマークをクリックして vESA にログインし、結果と関連するスキャン レポートを表示できます。dCloud セッションが完了するか期限切れになると、vESA と関連する Threat Analyzer レポートは利用できなくなります。セッションが完了するか期限切れになると、すべてのデータはスクラブされて dCloud から削除されます。

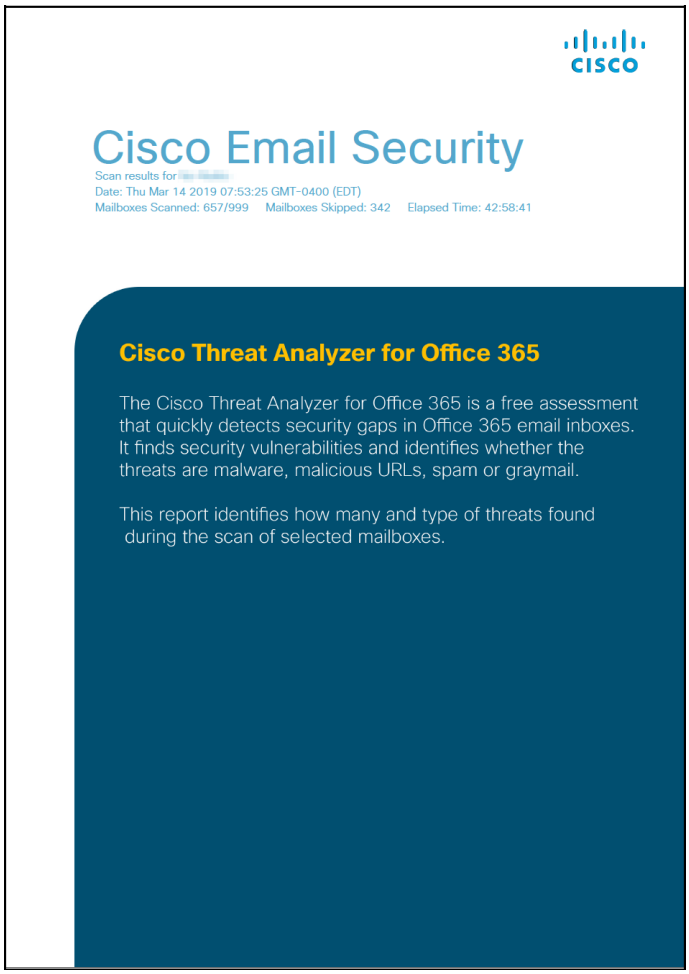
シナリオ 4： Threat Analyzer レポートの理解

価値提案：レポートの結果は、分かりやすいグラフィック表示形式です。

レポートの結果は、vESA 自体から一覧化されます。dCloud セッションが引き続きスケジュールされていて利用可能な間に、Google Chrome ブラウザの [Cisco vESA] ブックマークをクリックして vESA にログインし、結果と関連するスキャン レポートを表示できます。あるいは、ローカルのワークステーション/ラップトップから AnyConnect 経由で vESA にアクセスします（詳細については、このドキュメントの「トポロジ」と「はじめに」を参照してください)。

(*) vESA ユーザ インターフェイスを使い慣れていない場合は、dCloud から利用可能な **Cisco E メール セキュリティ インスタント デモ**をご覧ください。

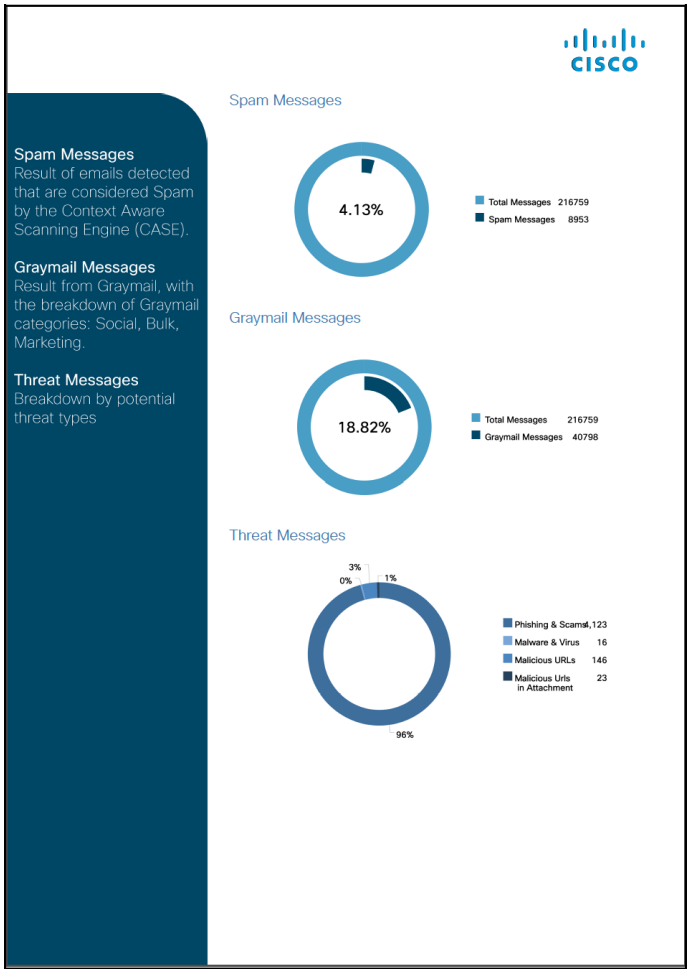
1/3 ページ



1 ページ目は、お客様向けレポートのカバー ページです。

ここには、スキャンされたメールボックスの数、スキップされたメールボックスの数、経過時間（スキャンの完了にかかった時間）などのスキャン結果の統計情報が記載されます。

2/3 ページ



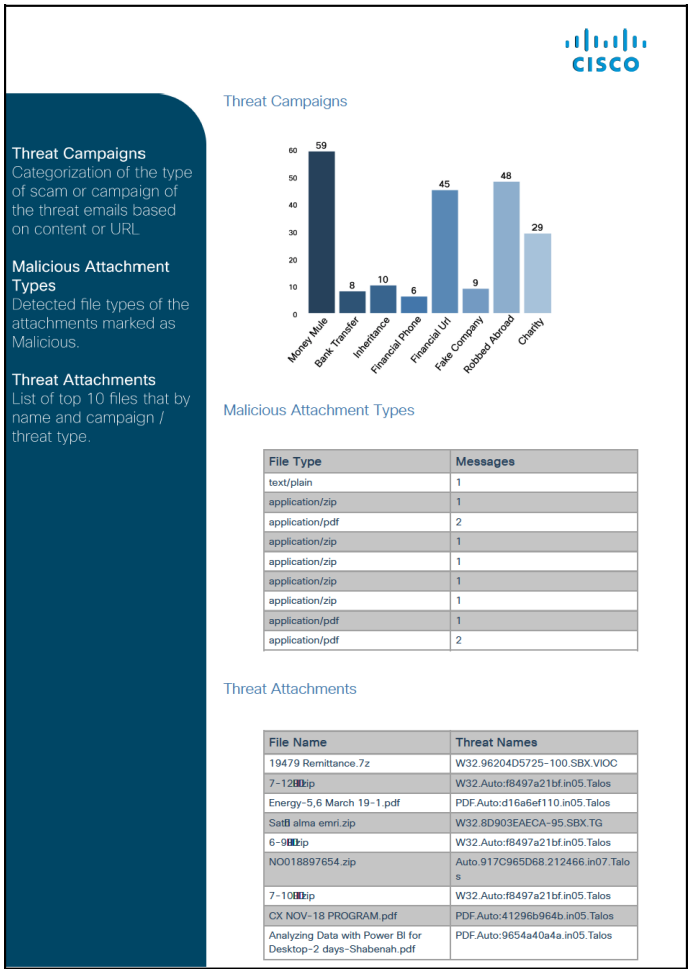
2 ページには、スパム、グレイメール、および脅威メッセージの割合が記載されます。

vESA の [概要（Overview）] > [着信メールの概要（Incoming Mail Summary）] の [Spam Detected（検出されたスパム）] に関連するスパム メッセージ。これらのメッセージの詳細を確認するには、[モニタ（Monitor）] > [着信メール（Incoming Mail）] を開き、[着信メールの詳細（Incoming Mail Details）] セクションをご覧ください。

vESA の [概要（Overview）] > [着信メールの概要（Incoming Mail Summary）] のマーケティング、ソーシャル ネットワーク、バルク メッセージに関連するグレイメール メッセージ。これらのメッセージの詳細を確認するには、[モニタ（Monitor）] > [着信メール（Incoming Mail）] を開き、[着信メールの詳細（Incoming Mail Details）] セクションをご覧ください。

脅威メッセージは、アウトブレイク フィルタによるスキャンの結果です。割合の詳細を確認するには、[モニタ（Monitor）] > [アウトブレイク フィルタ（Outbreak Filters）] を開き、[タイプ別の脅威（Threats by Type）]、[脅威の概要（Threat Summary）]、[脅威の詳細（Threat Details）] をご覧ください。

3/3 ページ



3 ページ目はアウトブレイク フィルタの詳細の続きです。[モニタ（Monitor）] > [アウトブレイク フィルタ（Outbreak Filters）] で表示される [脅威キャンペーン（Threat Campaigns）] と、[脅威の概要（Threat Summary）] のレビューが記載されます。

[モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] の [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] の表から、悪意のある添付ファイルのタイプが記載されます。

最後に、[モニタ（Monitor）] > [高度なマルウェア防御（Advanced Malware Protection）] の [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] の表から、脅威となる添付ファイルも記載されます（vESA の [高度なマルウェア防御（Advanced Malware Protection）] レポート ページと関連する表を表示することで、これらのファイルの完全な SHA を確認できます）。

vESA レポート

[例：vESA UI]

vESA の UI から、[モニタ（Monitor）] > <名前> の利用可能なレポートの大半を閲覧できます。

適切に配置されないレポートもあります。これは、Microsoft Azure/Microsoft O365 から Cisco Threat Analyzer ツールに API が開かれる際に、すべてのメールが vESA で 1 つの着信接続およびリスナーにバンドルされるためです。[モニタ（Monitor）] > [着信メール] の [着信メールの詳細（Incoming Mail Details）] の表で、[ドメイン情報なし（No Domain Information）] と関連するメール トラフィックの割合が 1 行しかないのはこのためです。

Cisco Threat Analyzer は、既存の O365 メールボックスの受信トレイのメッセージから、Cisco E メール セキュリティで検出可能なものを表示することのみを意図していることに注意してください。

Cisco E メール セキュリティの適切な**価値の実証（PoV）**に移行できるように、ツールで利用可能なサービス結果を活用してください。その後、お客様は接続レベル、セキュリティ スキャン、メール トラフィックの配信の結果を確認し、独自の Cisco E メール セキュリティ（CES）環境から、Cisco E メール セキュリティと Cisco Security Manager が提供する完全なレポート機能を表示して直接操作できます。

付録 A トラブルシューティング

ヒント：dCloud インスタンスの問題が発生した場合、dCloud セッションからサポート ケースを開いてください。

以下のトラブルシューティング ノートは、Microsoft Office 365 向け Cisco Threat Analyzer のページに記載されているものです。
https://docs.ces.cisco.com/docs/troubleshooting

注：すべてのシナリオが、dCloud からスケジュールおよび実行される Threat Analyzer ツール インスタンスに適用されるわけではありません。

Threat Analyzer ツールへのログイン時の API エラー

1. vESA のインターフェイス設定で、AsyncOS API（モニタリング）が AsyncOS API HTTP（6080）に対して有効になっていることを確認します。AsyncOS API HTTPS（6443）を有効にする必要はありません。
2. ネットワークおよび/またはファイアウォールを確認し、設定した IP アドレスに対してポート 6080 が許可されていることを確認します。ネットワーク アドレス変換（NAT）を使用している場合は、インターフェイスが適切にマッピングされていることを確認します。

Threat Analyzer ツールの UI にログイン中

- [ログイン中…（Logging In..）] のポップアップが回転する
- ページがロードされない

1. startofflinescan を実行することで CLI からスキャンを開始したことを確認します。
2. 適切なインターフェイスの IP アドレスでスキャンを開始したことを確認します。
3. Threat Analyzer ツールの実行に関する指示を確認します。

クレデンシャル検証中の API エラー

1. クライアント ID（アプリケーション ID）、テナント ID を確認します。アプリケーションの作成の手順で、Microsoft Azure からそれらを正確にコピーしたことを確認します。
2. 正しいサムプリントと、アプリケーションの作成の手順で使用したものと同じ .pem 証明書を使用していることを確認します。
3. offlinescan_logs を確認し、特定のエラーがないかどうかを確認します。

4. まれに最悪の場合、Microsoft Azure のアプリケーションが削除され、アプリケーションの作成の手順を再度実行する必要があります。

offlinescan_logs に以下が表示される。

- "Error while requesting token AADSTS90002: Tenant 'a2745a99-9999-999a-b999-cf78f467999a' not found. This may happen if there are no active subscriptions for the tenant. Check with your subscription administrator."

アプリケーション ID とテナント ID が逆になっていないかどうかを確認します。

offlinescan_logs に以下が表示される。

- "Error in requesting token: AADSTS70002: Error validating credentials. AADSTS50012: Client assertion is not within its valid time range."

以下のように、settime コマンドを使用して、vESA の CLI で手動で時間を調整します。

```
analyzer.lab> settime


WARNING: Changes to system time will take place immediately and do not require the user to run the
commit command.

Current time Thu Jan 17 15:27:06 2019 GMT.
Please enter the time in MM/DD/YYYY HH:MM:SS format.
[]> 01/18/2019 15:27:36

Time set to Fri Jan 18 15:27:36 2019 GMT.
```

通常は、時間を 1 日進めて設定することでエラーが修正されます。NTP サーバを設定している場合、NTP のポート（123）が vESA のネットワーク/ファイアウォールに対して開いていない可能性があります。

offlinescan_logs に以下が表示される。

- "Failed to connect to <name> mailbox with error Group not Exists"

[電子メールスキャン設定（Email Scan Setup）] ページに入力された LDAP グループ名を確認します。AD グループが存在することを確認する必要があります。Exchange 管理センターにログインして表示名を確認します。

offlinescan_logs に以下が表示される。

- "Tue Jan 15 19:25:58 2019 Info: Unable to read attachments(s) from the recipient's (sam@myexamplebank.com) mailbox"
- "Tue Jan 15 19:29:26 2019 Info: Skipping one message from the recipient's (sam@myexamplebank.com) mailbox since error ((552, 'size limit exceeded', u'tess@trainingcenterexample.com')) has occured"

これらは無視してかまいません。添付ファイルが破損しているか、大きすぎてスキャンできないか、スキャンがサポートされていません。「size limit exceeded」の場合は、単にメッセージのサイズが vESA がサポートするメールのサイズである 25 MB を超えていることを意味します。

offlinescan_logs に以下が表示される。

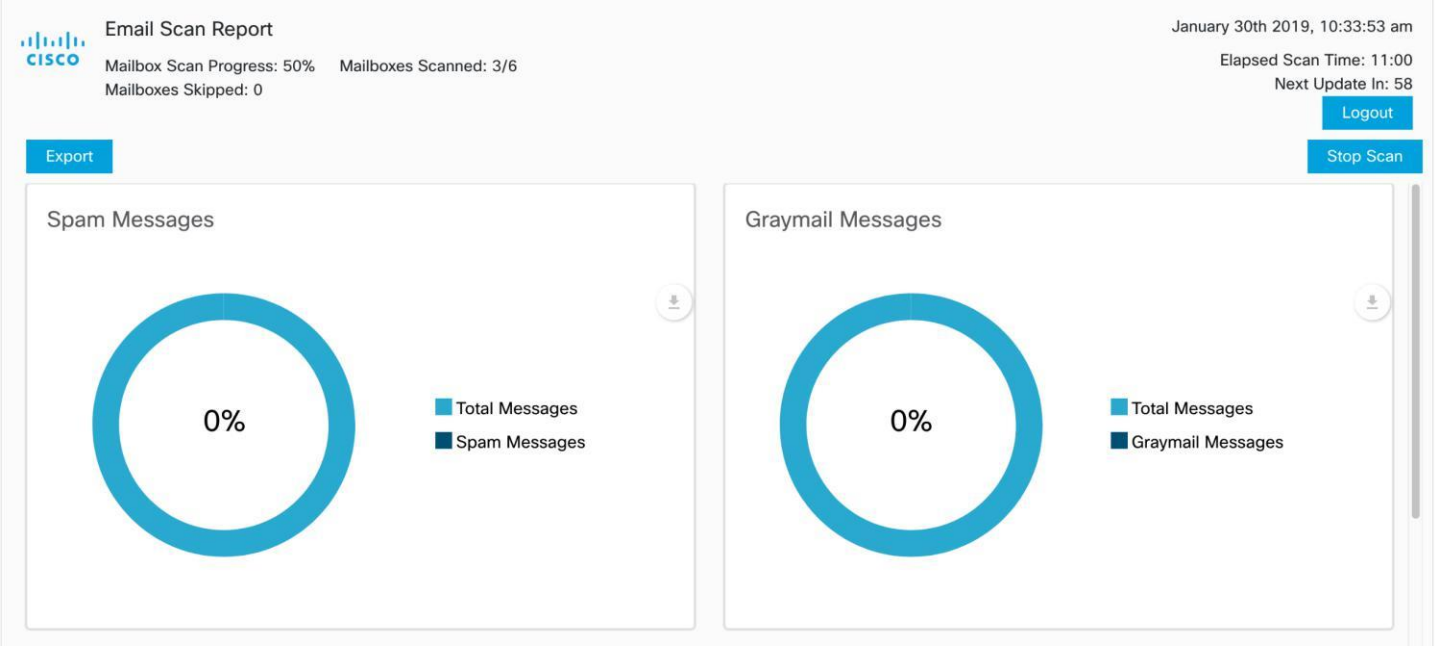
- "Failed to connect to %20joe@example.com mailbox with error User Not Exist"

スキャンするメールボックスのコンマ区切りの値を入力した場合、スペースが誤ってコピーされました。「%20」は、ASCII コードでスペースを表します。コンマ区切りのリストをスペースを含まないように再フォーマットしてください。

例：bob@example.com,joe@example.com

ダッシュボードに結果が表示されない

- スキャンが実行中で進行状況が表示されているものの、スパム、グレイメールなどの結果がダッシュボードに表示されない。



まずは、ゆっくり待ってください。Threat Analyzer は vESA に依存してレポートとメッセージのデータを使用し、ダッシュボードの結果と最終レポートを構築します。これには最低でも 1 時間かかります。

それでも 0 % の結果が続く場合、通常はファイアウォールおよび API ポート（6080）が原因です。vESA のネットワークおよびファイアウォール設定を確認してください。ポートが開いていることを確認してください。ポートを通過するトラフィックでレポート データが適切に許可されていない場合、ファイアウォールのリセットが必要な場合があります。

重要：dCloud インスタンスの問題が発生した場合、dCloud セッションからサポート ケースを開いてください。

ドキュメント タイプ

デモンストレーション ガイド

付録 B. よく寄せられる質問（FAQ）

FAQ はこのドキュメントに記載していません。Threat Analyzer ツールに関する最新の FAQ については、Microsoft Office 365 向け Cisco Threat Analyzer のページを参照してください。

https://docs.ces.cisco.com/docs/frequently-asked-questions-faq-threat-analyzer-tool

次のステップ

- Cisco E メール セキュリティの顧客評価を開始するには、https://order.ces.cisco.com/eval/ をご覧ください。
- Cisco E メール セキュリティの詳細は、http://www.cisco.com/web/JP/product/hs/security/emailsecurity/Products_Sub_Category_Home.html をご覧ください。

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