Cisco Threat Response との統合

この章は、次の項で構成されています。

アプライアンスと Cisco Threat Response との統合

アプライアンスを Cisco Threat Response と統合すると、Cisco Threat Response で次の操作を実行できます。

- 組織内の複数のアプライアンスから電子メール レポート、メッセージ トラッキング、および Web トラッキングのデータを確認します。
- 電子メールレポート、メッセージトラッキング、Web トラッキングで検出された脅威を特定、調査、および修正します。
- 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。
- 脅威をドキュメント化して調査内容を保存し、他のデバイスと情報を共有します。

（注） クラスタ化された設定では、ログイン中のアプライアンスはマシンモードの Cisco Threat Response にのみ登録できます。アプライアンスを Cisco Threat Response にスタンドアロンモードですでに登録している場合は、アプライアンスをクラスタに参加させる前に手動で登録を解除してください。

アプライアンスを Cisco Threat Response と統合するには、Cisco Threat Response にアプライアンスを登録する必要があります。

Cisco Threat Response には、次の URL のいずれかを使用してアクセスできます。

- https://visibility.amp.cisco.com
- https://visibility.eu.amp.cisco.com/

（注） 地域の URL（https://visibility.apjc.amp.cisco.com）を使用して Cisco Threat Response にアクセスした場合、現時点では Cisco Threat Response とアプライアンスの統合はサポートされていません。

始める前に

- 管理者アクセス権を使用して、Cisco Threat Response でユーザアカウントを作成していることを確認します。新しいユーザアカウントを作成するには、URL（https://visibility.amp.cisco.com）を使用して Cisco Threat Response のログインページに移動します。ログインページで [シスコ セキュリティ アカウントの作成（Create a Cisco Security account）] をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。
- Cisco Security Services Exchange（SSE）ポータルで Cisco Threat Response の統合が有効になっていることを確認します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動し、Cisco Threat Response と統合するモジュールに移動して、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。
- アプライアンスを Cisco Threat Response に登録する場合、ファイアウォールで HTTPS（インおよびアウト）443 ポートが次の FQDN に対してオープンになっていることを確認してください。
  - api-sse.cisco.com（アメリカ地域のユーザのみに対応）
  - api.eu.sse.itd.cisco.com（欧州連合（EU）のユーザのみに対応）

詳細については、ファイアウォール情報を参照してください。

手順

ステップ 1 アプライアンスにログインします。

ステップ 2 [ネットワーク（Networks）]>[クラウドサービス設定（Cloud Service Settings）] を選択します。

ステップ 3 [設定を編集（Edit Settings）] をクリックします。

ステップ 4 [有効（Enable）] チェックボックスをオンにします。

ステップ 5 アプライアンスを Cisco Threat Response に接続するために必要な Cisco Threat Response サーバを選択します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分が経過したら、[クラウドサービス設定（Cloud Service Settings）]ページに戻り、アプライアンスを Cisco Threat Response に登録します。

ステップ 8 Cisco Threat Response から登録トークンを取得し、アプライアンスを Cisco Threat Response に登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動

し、Cisco Threat Response と統合するモジュールに移動して、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

ステップ 9 Cisco Threat Response から取得した登録トークンを入力し、[登録（Register）] をクリックします。

ステップ 10 Cisco Threat Response への統合モジュールとしてアプライアンスを追加します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動し、Cisco Threat Response と統合するモジュールに移動して、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

次のタスク

Cisco Threat Response にアプライアンスを統合モジュールとして追加すると、Cisco Threat Response のアプライアンスから電子メールレポート、メッセージトラッキング、Web トラッキング情報を表示できます。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動し、Cisco Threat Response と統合するモジュールに移動して、[新しいモジュールの追加（Add New Module）] をクリックしてページに記載されている手順を参照してください。

（注） Cisco Threat Response からアプライアンス接続の登録解除するには、アプライアンスの [クラウドサービス設定（Cloud Services Settings）] ページで [登録解除（Deregister）] をクリックします。

ケースブックを使用した脅威分析の実行

事例集とピボットメニューは Cisco Threat Response で使用できるウィジェットです。

ケースブックは、調査および攻撃分析の際に主要な観測対象のグループを記録、整理、共有するために使用します。ケースブックを使用して、観測対象の現在の判定または傾向を取得できます。詳細については、https://visibility.amp.cisco.com/#/help/casebooks で Cisco Threat Response ドキュメントを参照してください。

ピボットメニューは、新しいケース、既存のケース、または Cisco Threat Response に登録されているその他のデバイス（AMP for Endpoints、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、攻撃分析に関する調査を行うために使用します。詳細については、https://visibility.amp.cisco.com/#/help/pivot-menus で Cisco Threat Response ドキュメントを参照してください。

E メール セキュリティ アプライアンスには、事例集とピボットメニューのウィジェットが搭載されるようになりました。[ケースブック（Casebook）] ウィジェットと [ピボット メニュー（Pivot Menu）] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。

- 観測対象をケースブックに追加し、脅威分析の調査を実行します。

- 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、脅威分析のために調査します。

次にこのリリースでサポートされている観測対象のリストを示します。

- IP アドレス
- ドメイン
- URL
- ファイル ハッシュ（SHA-256 のみ）

（注）
- ピボット メニュー ウィジェットは、アプライアンスの電子メールレポートページで、監視対象の横にあります。
- 事例集ウィジェットは、アプライアンスの電子メールレポートページの右下隅にあります。

関連項目

- クライアント ID およびクライアント パスワード クレデンシャルの取得 （4 ページ）
- 攻撃分析のケースブックへ観測対象を追加 （6 ページ）

クライアント ID およびクライアント パスワード クレデンシャルの取得

アプライアンスのケースブックとピボット メニュー ウィジェットにアクセスするには、クライアント ID とクライアント パスワードが必要です。

始める前に

次の「はじめる前に」セクションに記載されているすべての前提条件を満たしていることを確認してください。 アプライアンスと Cisco Threat Response との統合 （1 ページ）

手順

ステップ 1 アプライアンスの新しい Web インターフェイスにログインします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセスを参照してください。

ステップ 2 **[ケースブック（Casebook）]** ボタンをクリックします。

ステップ 3 新しい API クライアントを追加します。

a) **[Threat Response APIクライアント（Threat Response API Clients）]** リンクをクリックします。

[Threat Response APIクライアント（Threat Response API Clients）] リンクをクリックすると、Cisco Threat Response ログインページにリダイレクトされます。

b) Cisco Threat Response にログインします。
c) **[APIクレデンシャルの追加（Add API Credentials）]** をクリックします。
d) アプライアンス名（「Email_Security_Appliance」など）をクライアント名として入力します。
e) ケースブックとピボット メニュー ウィジェットへのフル アクセスを付与する次のスコープを選択します。

- ケースブック（Casebook）
- 強化（Enrich）
- プライベート インテリジェンス（Private Intelligence）
- 応答（Response）
- 検査（Inspect）

（注）
- ケースブック ウィジェットにのみアクセスする場合は、[ケースブック（Casebook）]、[プライベートインテリジェンス（Private Intelligence）]、および [検査（Inspect）] をスコープとして選択します。
- ピボット メニュー ウィジェットにのみアクセスする場合は、[強化（Enrich）] および [応答（Response）] をスコープとして選択します。

f) [新しいクライアントの追加（Add New Client）] をクリックします。
g) クライアント ID とクライアント パスワードをクリップボードにコピーします。

（注） [新しいクライアントの追加（Add New Client）] ダイアログ ボックスを閉じる前に、クライアント ID とクライアント パスワードをメモしてください。

h) [閉じる（Close）] をクリックします。

（注） 新しい API クライアントを追加する場合は、既存の API クライアントを削除する必要はありません。

ステップ 4 アプライアンスの [ログインしてケースブック/ピボットメニューを使用（Login to use Casebook/Pivot Menu）] ダイアログ ボックスのステップ 3 で取得したクライアント ID とクライアント パスワードを入力します。

ステップ 5 [ログインしてケースブック/ピボットメニューを使用（Login to use Casebook/Pivot Menu）] ダイアログ ボックスで必要な Cisco Threat Response サーバを選択します。

ステップ 6 [認証（Authenticate）] をクリックします。

（注） クライアント ID、クライアント パスワード、および Cisco Threat Response サーバを編集する場合は、[ケースブック（Casebook）]  ボタンを右クリックして詳細を追加します。

次のタスク

観測対象をケースブックに追加し、攻撃分析の調査を実行します。（「攻撃分析のケースブックへ観測対象を追加 （6 ページ）」を参照）。

攻撃分析のケースブックへ観測対象を追加

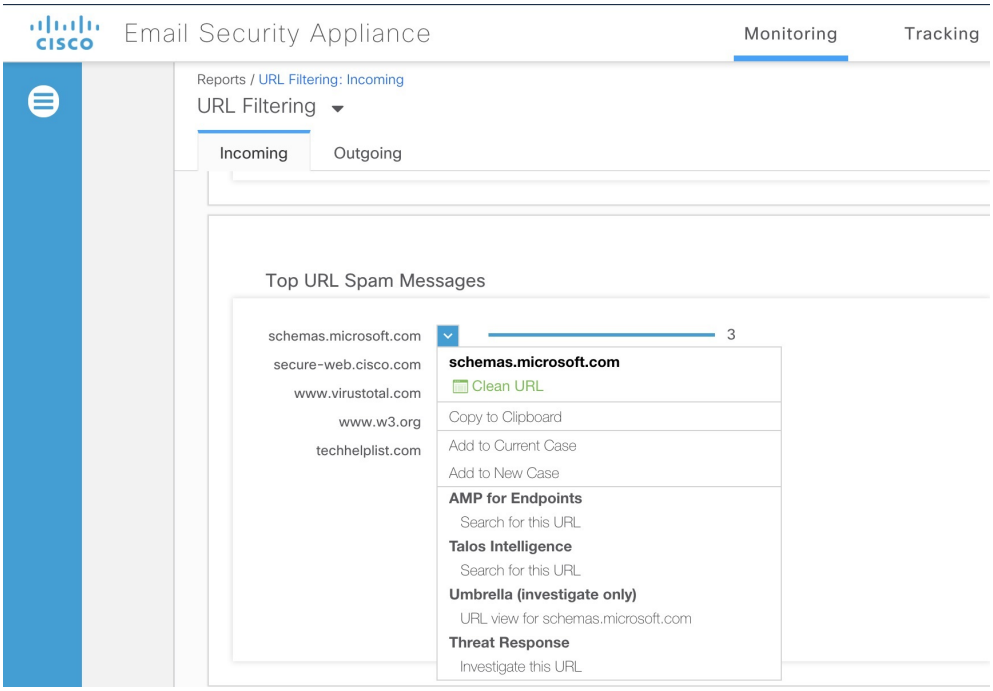
始める前に

アプライアンスのケースブックとピボット メニュー ウィジェットにアクセスするには、クライアント ID とクライアント パスワードを取得します。詳細については、クライアント ID およびクライアント パスワード クレデンシャルの取得 （4 ページ）を参照してください。

手順

ステップ 1 アプライアンスの新しい Web インターフェイスにログインします。詳細については、Web ベースのグラフィカル ユーザー インターフェイス（GUI）へのアクセスを参照してください。

ステップ 2 [電子メールレポート（Email Reporting）] ページに移動して、該当する観測対象（schemas.micrsoft.com など）の横にあるピボットメニュー ボタンをクリックし、[新しいケースに追加（Add to New Case）] または [現在のケースに追加（Add to Current Case）] をクリックします。



（注）

- 観測対象の横にあるドラッグ アンド ドロップ ボタンを使用して、観測対象を既存のケースへドラッグ アンド ドロップします。
- ピボット メニュー ボタンを使用して、ポータルに登録された他のデバイスの観測対象（AMP for Endpoints など）をピボットし、攻撃分析の調査を実行します。

ステップ 3 [ケースブック（Casebook）] ボタンをクリックして、観測対象が新しいまたは既存のケースに追加されたかを確認します。

ステップ 4 **（オプション）** ボタンをクリックして、タイトル、説明、またはメモをケースブックに追加します。

ステップ 5 [このケースを調査（Investigate this Case）] をクリックして、攻撃分析の観測対象を調査します。詳細については、https://visibility.amp.cisco.com/#/help/introduction で Cisco Threat Response のマニュアルを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。