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

この章で説明する内容は、次のとおりです。

- Cisco Threat Response との統合
- CLI を使用した Cisco Threat Response へのアプライアンスの統合
- ケースブックを使用した脅威分析の実行

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データを表示します。
- 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。

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 を使用してアクセスできます。

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

Cisco Threat Response との統合

（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 に移動して、Cisco Threat Response と統合するモジュールを選択し、[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.eu.sse.itd.cisco.com（欧州連合（EU）のユーザのみに対応）
  - api-sse.cisco.com（ アメリカ地域のユーザのみに対応）
  - est.sco.cisco.com（APJC、EU、および NAM ユーザに対応）

詳細については「Firewall Information」 を参照してください。

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 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [有効（Enable）] 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 に移動して、Cisco Threat

Response と統合するモジュールを選択し、[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 に移動して、Cisco Threat Response と統合するモジュールを選択し、[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 CLI コマンドを使用して、アプライアンスを Cisco Threat Response と統合できます。

- `threatresponseconfig`：このコマンドを使用して、アプライアンスで Cisco Threat Response 機能を設定します。
- `cloudserviceconfig`：このコマンドを使用して、アプライアンスに Cisco Threat Response 機能を登録します。

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、Web レポート、メッセージ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 に移動して、Cisco Threat Response と統合するモジュールを選択し、[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） アプライアンスの接続を Cisco Threat Response から登録解除するには、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。

- Cisco Threat Response で Web モジュールを設定できるようになりました。

  Cisco Threat Response で、[設定（Settings）] > [統合モジュール（Integration Modules）] > [モジュールの設定（Configure Modules）] > [SMA Web-シスコのコンテンツセキュリティ管理アプライアンス-Web（SMA Web-Cisco Content Security Management Appliance-Web）] に移動します。

  詳細については、https://visibility.amp.cisco.com/?beta-modules=1を参照してください。

  （注） この機能はまだベータ版です。

- 別の Cisco Threat Response サーバ（欧州用の「api.eu.sse.itd.cisco.com」など）に切り替える場合は、最初に Cisco Threat Response からアプライアンスの登録を解除して、「アプライアンスと Cisco Threat Response との統合」のステップ 1 ～ 9 を実行する必要があります。

（注） Cisco Threat Response とアプライアンスを統合した後は、電子メールと Web のレポート機能が集中管理されるため、電子メール セキュリティ アプライアンスを Cisco Threat Response に統合する必要はありません。

CLI を使用した Cisco Threat Response へのアプライアンスの統合

ここでは、次の CLI コマンドについて説明します。

threatresponseconfig

説明

`threatresponseconfig` コマンドは次の目的で使用します。

- アプライアンスの Cisco Threat Response 機能を有効にします。
- アプライアンスの Cisco Threat Response 機能を無効にします。

使用法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

バッチ コマンド：このコマンドはバッチ形式をサポートしています。

例

次の例では、`threatresponseconfig` コマンドを使用してアプライアンスの Cisco Threat Response 機能を有効にします。

```
mail1.example.com> threatresponseconfig

Choose the operation you want to perform:
- ENABLE - To enable the Cisco Threat Response feature on your appliance.

[]> enable

The Cisco Threat Response feature is currently enabled on your appliance. Use the
cloudserviceconfig command to register your appliance with the Cisco Threat
Response portal.

mail1.example.com> commit

Please enter some comments describing your changes:
[]>
```

```
Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

次の例では、threatresponseconfig コマンドを使用してアプライアンスの Cisco Threat Response 機能を無効にします。

```
mail1.example.com> threatresponseconfig

Choose the operation you want to perform:
- DISABLE - To disable the Cisco Threat Response feature on your appliance.
[]> disable

The Cisco Threat Response feature is currently disabled on your appliance.

mail1.example.com> commit

Please enter some comments describing your changes:
[]>

Changes committed: Mon Nov 19 10:04:35 2018 GMT
```

cloudserviceconfig

説明（Description）

cloudserviceconfig コマンドは次の目的で使用します。

- Cisco Threat Response ポータルにアプライアンスを登録します。
- Cisco Threat Response ポータルからアプライアンスを登録解除します。
- アプライアンスを Cisco Threat Response ポータルに接続するための Cisco Threat Response サーバを選択します。

使用法

確定：このコマンドに commit は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

バッチ コマンド：このコマンドはバッチ形式をサポートしています。

例

次の例では、cloudserviceconfig コマンドを使用してアプライアンスを Cisco Threat Response ポータルに登録できます。

```
mail1.example.com> cloudserviceconfig

Choose the operation you want to perform:

- REGISTER - To register the appliance with the Cisco Threat Response portal.
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.
[]> register

Enter a registration token key to register your appliance with the Cisco Threat
Response portal.
[]> de7c55f3ff0absdfsf4a25aae94dfb064642
```

```
The appliance registration is in progress.
```

次の例では、cloudserviceconfig コマンドを使用して、アプライアンスを Cisco Threat Response ポータルに接続するための Cisco Threat Response サーバを選択します。

```
mail1.example.com> cloudserviceconfig

Choose the operation you want to perform:
- DEREGISTER - To deregister the appliance from the Cisco Threat Response
portal.
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.
[]> settrs

Available list of Threat Response Servers:

1.
2. EUROPE (api.eu.sse.itd.cisco.com)
3.AMERICAS (api-sse.cisco.com)

Enter threat response server to connect to the Cisco Threat Response portal.:
[]> 2

Selected threat response server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.

mail1.example.com> commit
Please enter some comments describing your changes:
[]>

Changes committed: Mon Jum 19 10:04:35 2019 GMT
```

次の例では、cloudserviceconfig コマンドを使用して、Cisco Threat Response ポータルからアプライアンスの登録を解除します。

```
mail1.example.com> cloudserviceconfig

The Content Security Management appliance is successfully registered with the
Cisco Threat Response portal.

Choose the operation you want to perform:
- DEREGISTER - To deregister the appliance from the Cisco Threat Response
portal.
-SETTRS - Set the Threat Response Server to connect to the Cisco Threat Response portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Threat Response portal.

If you deregister, you will not be able to access the Cloud Service features. [N]> yes

The Content Security Management appliance deregistration is in progress.
```

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。

コンテンツ セキュリティ管理アプライアンスで、ケースブックとピボット メニューのウィジェットが使用でき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、Web レポートページ、およびトラッキングページの観測対象の横にあります。
- 事例集ウィジェットは、Cisco SecureX リボンの一部です。

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

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。 Cisco Threat Response との統合 （1 ページ）

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 インターフェイスへのアクセス」を参照してください。Web インターフェイスへのアクセス

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) アプライアンスの名前（「Management_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 （9 ページ） を参照してください。

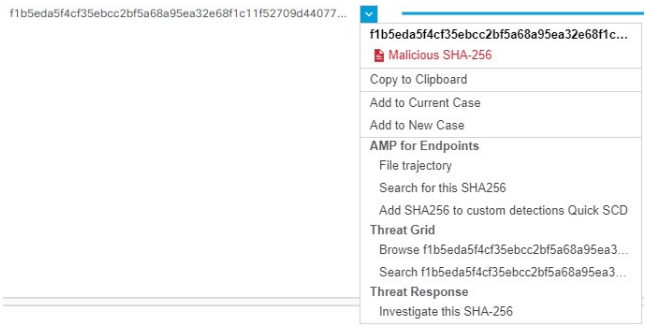
攻撃分析のケースブックへ観測対象を追加

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 （7 ページ）を参照してください。

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 インターフェイスへのアクセス」を参照してください。https://www.cisco.com/c/en/us/td/docs/security/security_management/sma/sma13-6-1/User-Guide/b_SMA_Admin_Guide_13_6_1/b_NGSMA_Admin_Guide_chapter_01.html#task_1280297

ステップ 2 [メールレポート（Email Reporting）] または [Web レポート（Web Reporting）] ページへ移動して、該当する観測対象（bit.ly 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。



- 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 [事例集（Casebook）] ボタンをクリックして、観測対象が新しいケース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。