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。

- アプライアンスと Cisco Threat Response との統合 （1 ページ）
- ケースブックを使用した脅威分析の実行 （3 ページ）
- Cisco Success Network を使用した Cisco Web セキュリティアプライアンスのユーザーエクスペリエンスの向上 （7 ページ）

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 Webトラッキングデータを表示します。
- Web トラッキングで確認された脅威を特定し、調査し、修復します。
- 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。
- ポータルで脅威をドキュメント化して調査を保存し、ポータル内の他のデバイス間で情報を共有します。

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 （北米）
- https://visibility.eu.amp.cisco.com （欧州）
- https://visibility.apjc.amp.cisco.com （アジア太平洋、日本、中国）

（注） アプライアンスで CTR を有効にして登録している場合、アプライアンスは自動的にシスコへの Cisco Success Network（CSN）テレメトリデータの送信を開始します。「Cisco Success Network を使用した Cisco Web セキュリティアプライアンスのユーザーエクスペリエンスの向上」を参照してください。

始める前に

- CLI にアクセスし、**reportingconfig**>**CTROBSERVABLE** コマンドを有効にします。このコマンドを使用して CTR の監視可能なインデックスを有効にすると、ユーザーがアクセスした URL のインデックスを作成できます。また、アプライアンス トラッキング データベース内の URL を検索する粒度も提供されます。
- Cisco Threat Response にアクセスするには、シスコのセキュリティ ユーザー アカウントが必要です。組織内のユーザーにシスコのセキュリティアカウントがある場合は、システム管理者にお問い合わせください。シスコのセキュリティ ユーザー アカウントをお持ちでない場合は、Cisco Threat Response のログインページで作成できます。管理者アクセス権を使用して、Cisco Threat Response でユーザーアカウントを作成していることを確認します。新しいユーザーアカウントを作成するには、北米の場合は https://visibility.amp.cisco.com、欧州の場合は https://visibility.eu.amp.cisco.com を使用して Cisco Threat Response のログインページに移動し、ログインページで [シスコの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、北米の場合は https://visibility.amp.cisco.com/help/module-wsa 、欧州の場合は https://visibility.eu.amp.cisco.com/help/module-wsa にある Cisco Threat Response のマニュアルを参照してください。
- Cisco Threat Response にアプライアンスを登録するには、ファイアウォール上で HTTPS（アウトバウンド）443 ポートを次の FQDN 用に開い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）
  - api.apj.sse.itd.cisco.com（APJC ユーザのみに対応）
  - est.sco.cisco.com（アメリカ地域と EU 両方の APJC ユーザに対応）
- DNS サーバーが管理（M1）インターフェイスに設定されているホスト名を解決できることを確認します。

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 変更を送信し、保存します。

ステップ 6 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 7 [脅威対応サーバー（Threat Response Server）] ドロップダウンリストから希望するサーバーを選択します。

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、北米の場合は https://visibility.amp.cisco.com/help/module-wsa 、欧州の場合は https://visibility.eu.amp.cisco.com/help/module-wsa にある Cisco Threat Response のマニュアル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、北米の場合は https://visibility.amp.cisco.com/help/module-wsa 、欧州の場合は https://visibility.eu.amp.cisco.com/help/module-wsa にある Cisco Threat Response のマニュアルを参照してください。

次のタスク

Cisco Threat Response で統合モジュールとしてアプライアンスを追加した後は、Cisco Threat Response でアプライアンスから Web トラッキング情報を確認できます。詳細については、北米の場合は https://visibility.amp.cisco.com/help/module-wsa、欧州の場合は https://visibility.eu.amp.cisco.com/help/module-wsa にある Cisco Threat Response のマニュアル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。

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、北米の場合は https://visibility.amp.cisco.com/help/casebooks、欧州の場合は https://visibility.eu.amp.cisco.com/help/casebooks にある Cisco Threat Response のマニュアルを参照してください。

ピボットメニューは、Web セキュリティ アプライアンス インターフェイスから、観測対象に対して直接的に脅威対応可能なタスクを実行するために使用されます。これらのタスクは、Cisco Threat Response または任意のユーザー設定モジュール（AMP for Endpoints、Cisco Umbrella、Cisco Talos Intelligence など）を使用して実行できます。詳細については、北米の場合は

https://visibility.amp.cisco.com/help/pivot-menus、欧州の場合は https://visibility.eu.amp.cisco.com/help/pivot-menus にある Cisco Threat Response のマニュアルを参照してください。

Web セキュリティアプライアンスには、ケースブックとピボットメニューのウィジェットが含ま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。

Web セキュリティアプライアンスのユーザーインターフェイスに Cisco Threat Response のピボットメニューがある観測対象のリストを以下に示します。

- 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 Web レポートページの観測対象の横にあります。
- ケースブック ウィジェットは、アプライアンスの Web レポートページの右下隅にあります。

関連トピック

- 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）

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。

ステップ 2 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) [Threat Response] で、[設定（Settings）] をクリックし、[APIクライアント（API Clients）] を選択して [APIクライアント（API Clients）] ページに移動します。

d) **[APIクレデンシャルの追加（Add API Credentials）]** をクリックします。

e) アプライアンスの名前（「Web_Security_Appliance」など）をクライアント名として入力します。

f) 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。

g) [新しいクライアントの追加（Add New Client）] をクリックします。

h) 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。

i) [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 3 **[ケースブック（Casebook）]** ボタンをクリックします。

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 2 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 （4 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。

ステップ 2 [Web レポート（Web 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、Cisco Threat Response またはその他の設定済み Cisco Threat Response モジュールを使用した観測対象で脅威対応が有効なアクション（Umbrella を使用したドメインのブロック、AMP を使用したファイルハッシュのブロック、すべてのモジュールを同時に使用した IP の調査など）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、北米の場合は https://visibility.amp.cisco.com/help/introduction 、欧州の場合は

https://visibility.eu.amp.cisco.com/help/introduction にある Cisco Threat Response のマニュアルを参照してください。

Cisco Success Network を使用した Cisco Web セキュリティアプライアンスのユーザーエクスペリエンスの向上

概要

Cisco Success Network（CSN）機能を使用して、アプライアンスや機能の使用状況の詳細をシスコに送信できます。シスコはこれらの詳細情報を使用して、デバイス情報、無料の機能やライセンス供与された機能のリスト、およびそれらのアクティベーション ステータスを識別します。

アプライアンスや機能の使用状況の詳細をシスコに送信する機能により、組織は次のことを行うことができます。

- 収集されたテレメトリデータの分析を実行し、デジタルキャンペーンを使用してユーザに推奨事項を提示することによって、ユーザネットワークでの製品の有効性を向上させます。
- Cisco Web セキュリティアプライアンスの使用により、ユーザーエクスペリエンスが向上します。

次の表に、シスコに送信されるアプライアンスと機能の使用状況の詳細情報のサンプルデータを示します。

アプライアンスの詳細

- x90、x95、100v、300v、600v などのアプライアンスモデル。
- アプライアンスのシリアル番号とソフトウェアバージョン。
- アプライアンスのインストール日。
- 一意のデバイス識別子

機能の詳細

- 機能の名前。
- 有効になっている機能のリスト。
- 機能のステータス（準拠しているか、していないか）。
- 失効日
- 機能 ID

サンプルデータ

（注） シスコに送信されるテレメトリデータを検証するには、*csid_logs* および *sse_connectord_log* のログ サブスクリプション レベルをトレースモードにする必要があります。

トレースモードの *sse_connectord_log.current* で詳細を表示できます。


```
Thu May XX 10:48:30 2020 Trace: {
    "version": "0.X",
    "payload": {
        "recordVersion": "X.0",
        "recordedAt": 1589453310965,
        "deviceInfo": {
            "slVAN": "WSA",
            "installDate": 1589269184000,
            "version": "12.5.0-XXX",
            "userAccountID": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
            "model": "S600x",
            "udi": "XXXXXXXXXXXXXXXXXXXX-XXXXXXXXXXXX"
        },
        "recordType": "CST_WSA",
        "features": {
            "free": [
                {
                    "enabled": "Y",
                    "featureName": "Smart Software Licensing"
                },
                {
                    "enabled": "N",
                    "featureName": "Identity Services Engine"
                },
                {
                    "enabled": "Y",
                    "featureName": "Cloud Services"
                },
                {
                    "enabled": "N",
                    "featureName": "Proxy Auto-Configuration File Hosting"
                },
                {
                    "enabled": "N",
                    "featureName": "Local Reporting Service"
                },
                {
                    "enabled": "Y",
                    "featureName": "Centralized Reporting Service"
                }
            ],
            "licensed": [
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Cisco Web Usage Controls",
                    "featureID":
"regid.2018-05.com.cisco.WSA-WUC,1.0_6e3a0734-ef40-4c60-bbcd-66ea1796231d",
                    "expiry": 1591803862000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus Webroot",
                    "featureID":
```

```
"regid.2018-05.com.cisco.WSA-AMW,1.0_794905fe-57e0-44df-8056-c1fc54f968d2",
                    "expiry": 1591803867000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance L4 Traffic Monitor",
                    "featureID":
"regid.2018-05.com.cisco.WSA_SB,1.0_c4b92628-15a4-4b73-94ad-9db1383054ce",
                    "expiry": 1591803872000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "N",
                    "featureName": "Web Security Appliance Cisco AnyConnect SM for
AnyConnect",
                    "featureID":
"regid.2018-05.com.cisco.WSA_MUS,1.0_d3f3389a-cdc4-48e3-bc84-8b590ea2d908",
                    "expiry": 1591803877000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Advanced Malware protection
Reputation",
                    "featureID":
"regid.2018-05.com.cisco.WSA_AMPREPU,1.0_a51bae61-c688-475a-aa19-51f86b52671e",
                    "expiry": 1591803893000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus Sophos",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMS,1.0_fda29c84-e1e7-4bb5-a220-f872e67bc44d",
                    "expiry": 1591803908000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Web Reputation Filters",
                    "featureID":
"regid.2018-05.com.cisco.WSA-WREP,1.0_37bb916e-65e2-4a55-ab3e-262d290c020a",
                    "expiry": 1591803857000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                   "featureName": "Web Security Appliance Advanced Malware Protection",

                    "featureID":
"regid.2018-05.com.cisco.WSA-AMP,1.0_34331e7c-0be5-4898-8563-a69c0a5fefba",
                    "expiry": 1591803882000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Anti-Virus McAfee",
                    "featureID":
"regid.2018-05.com.cisco.WSA-AMM,1.0_b8354876-14f5-4285-8dea-ca6a2bfb74c4",
                    "expiry": 1591803898000
                },
                {
                    "status": "IN_COMPLIANCE",
```

```
                    "enabled": "Y",
                    "featureName": "Web Security Appliance Web Proxy and DVS Engine",
                    "featureID":
"regid.2018-05.com.cisco.WSA_WP,1.0_996c8b90-5305-43de-bdb8-bf48aa9d0457",
                    "expiry": 1591803903000
                },
                {
                    "status": "OUT_OF_COMPLIANCE",
                    "enabled": "N",
                    "featureName": "Web Security Appliance HTTPs Decryption",
                    "featureID":
"regid.2018-05.com.cisco.WSA_WD,1.0_563c38e7-7633-4cdc-a79f-3871d1284b57",
                    "expiry": 1591803887000
                }
            ]
        }
    },
    "metadata": {
        "topic": "wsa.telemetry",
        "contentType": "application/json"
    }
}
```


関連項目

- アプライアンスでの Cisco Success Network の有効化と登録 （10 ページ）。
- Cisco Success Network の無効化 （11 ページ）。

アプライアンスでの Cisco Success Network の有効化と登録

始める前に

アプライアンスが Cisco Threat Response に登録されていることを確認します。アプライアンスと Cisco Threat Response との統合 （1 ページ）を参照してください。

ステップ 1 [ネットワーク（Network）] > [クラウドサービス設定（Cloud Service Settings）] に移動します。

ステップ 2 [設定（Settings）] セクションで、[設定の編集（Edit Settings）] をクリックし、[Threat Response] の横にある [有効化（Enable）] チェックボックスをオンにします。

ステップ 3 [登録（Registration）] セクションで、次の手順を実行します。

a) ドロップダウンリストから適切な脅威対応サーバーを選択します。

- 米国（api-sse.cisco.com）
- 欧州（api.eu.sse.itd.cisco.com）
- アジア太平洋、日本、中国（api.apj.sse.itd.cisco.com）

a) Security Service Exchange（SSE）ポータルを介して生成された登録トークンを入力します。

SSE ポータルにアクセスして登録用のトークンを生成する必要があります。

b) [登録（Register）] をクリックします。

ステップ 4 変更を送信し、保存します。

Cisco Threat Response ポータルからアプライアンスの登録を解除するには、[登録解除（Deregister）] をクリックします。

Cisco Success Network の無効化

ステップ 1 [システム管理（System Administration）] > [Cisco Success Network] に移動します。

ステップ 2 [Cisco Network Success] の下にある [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [Cisco Success Network] の横にある [有効化（Enable）] チェックボックスをオフにします。

ステップ 4 変更を送信し、保存します。

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。