Cisco SecureX および 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 SecureX または Cisco Threat Response の統合

Cisco SecureXは、すべてのシスコセキュリティ製品に組み込まれたセキュリティプラットフォームです。これは新しいテクノロジーを導入する必要のないクラウドネイティブです。Cisco SecureX は、可視性を統合し、自動化を可能にして、ネットワーク、エンドポイント、クラウド、およびアプリケーション全体のセキュリティを強化するプラットフォームを提供することで、脅威からの保護の要求を簡素化します。統合プラットフォームで技術を連携することで、Cisco SecureXは測定可能な分析情報、望ましい成果、比類のないチーム間のコラボレーションを実現します。Cisco SecureX では、セキュリティ インフラストラクチャを連携させて機能を拡張できます。

アプライアンスと Cisco SecureX または Cisco Threat Response の統合には、次のセクションが含まれています。

アプライアンスを Cisco SecureX または Cisco Threat Response と統合し、Cisco SecureX または Cisco Threat Response で以下のアクションを実行できます。

- 組織内の複数のアプライアンスから Web データを表示および送信します。
- Web レポートおよびトラッキングで検出された脅威を特定、調査、修正します。
- 侵害された URL または Web トラフィックをブロックします。
- 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。
- 悪意のあるドメインのブロック、不審な観測対象の追跡、承認ワークフローの開始、または Web ポリシーを更新するための IT チケットの作成を行います。

Cisco SecureX または Cisco Threat Response には、次の URL を使用してアクセスできます。

https://securex.us.security.cisco.com/login

Cisco Web セキュリティアプライアンス は高度な脅威防御機能を備え、脅威を迅速に検出、ブロック、修復します。また、データの損失を防ぎ、送信中の重要情報をエンドツーエンドの暗号化によって保護します。Web セキュリティアプライアンス モジュールで強化できる観測対象の詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動し、Cisco SecureX と統合するモジュールに移動して、[詳細情報（Learn More）] をクリックしてください。

アプライアンスと Cisco SecureX または Cisco Threat Response の統合方法

表 *1*: アプライアンスと *Cisco SecureX* または *Cisco Threat Response* の統合方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 （3 ページ）
ステップ 2	Web セキュリティアプライアンス で、Cisco SecureX または Cisco Threat Response の統合を有効にします。	Cisco Web セキュリティアプライアンス での Cisco SecureX または Threat Response の統合の有効化 （4 ページ）
ステップ 3	Cisco SecureX で、アプライアンスをデバイスとして追加し、登録して、登録トークンを生成します。	詳細については、次を参照してください。https://securex.us.security.cisco.com/help/settings-devices
ステップ 4	Web セキュリティアプライアンス で、Cisco SecureX または Cisco Threat Response の登録を完了します。	Cisco Web セキュリティアプライアンス での Cisco SecureX または Cisco Threat Response の登録 （4 ページ）

	操作内容	詳細
ステップ 5	登録が成功したかどうかを確認します。	登録が成功したかどうかの確認 （5 ページ）
ステップ 6	Cisco SecureX で、Web セキュリティ アプライアンス モジュールを追加します。	詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX と統合するために必要な Web セキュリティアプライアンス 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。

前提条件

（注） すでに Cisco Threat Response ユーザアカウントを持っている場合は、Cisco SecureX ユーザアカウントを作成する必要はありません。Cisco Threat Response ユーザアカウントのクレデンシャルを使用して Cisco SecureX にログインできます。

- 管理者アクセス権を使用して、Cisco SecureX 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://securex.us.security.cisco.com/login）を使用して **Cisco SecureX のログイン**ページに移動し、ログインページで [SecureXサインオンアカウントの作成（Create a SecureX Sign-on 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。
- （プロキシサーバを使用していない場合のみ）アプライアンスを Cisco SecureX または 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（NAM 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（APJC、EU、および NAM ユーザに対応）

Cisco Web セキュリティアプライアンスでの Cisco SecureX または Threat Response の統合の有効化

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）]** 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 SecureX または Cisco Threat Response に接続するために必要な Cisco SecureX または Cisco Threat Response サーバーを選択します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、[登録（Register）] ボタンがアプライアンスに表示されるかどうかを確認します。

次のタスク

アプライアンスを Cisco SecureX または 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 SecureX 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。

Cisco Web セキュリティアプライアンスでの Cisco SecureX または Cisco Threat Response の登録

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 [クラウドサービス設定（Cloud Services Settings）] に、登録トークンを入力し、[登録（Register）] をクリックします。

（注） CLI を使用して Cisco SecureX または Cisco Threat Response を登録するには、`cloudserviceconfig` コマンドを使用します。

次のタスク

登録が成功したかどうかの確認 （5 ページ）

登録が成功したかどうかの確認

- Security Services Exchange で、Security Services Exchange のステータスを確認して、正常に登録されたことを確認します。
- Cisco SecureX で、[デバイス（Devices）] ページに移動し、Security Services Exchange に登録されている Web セキュリティアプライアンス を表示します。

（注） 別の Cisco SecureX サーバーまたは Cisco Threat Response サーバー（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 SecureX または 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 SecureX または Cisco Threat Response の統合方法 （2 ページ）のステップを実行する必要があります。

アプライアンスを Cisco SecureX または Cisco Threat Response と統合した後は、Cisco Security Management アプライアンスを Cisco SecureX または Cisco Threat Response と統合する必要はありません。

Security Services Excange にアプライアンスが正常に登録されたら、Cisco SecureX に Web セキュリティアプライアンス Web モジュールを追加します。詳細については、https://securex.us.security.cisco.com/settings/modules/availableに移動して、Cisco SecureX 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。

Web セキュリティアプライアンスでの Cisco Cloud Services ポータルの有効化

ステップ 1 Web セキュリティアプライアンス 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 **[有効（Enable）]** をクリックします。

ステップ 4 [Cisco Cloud Servicesの有効化（Enable Cisco Cloud Services）] チェックボックスをオンにします。

ステップ 5 必要な Cisco Secure サーバーを選択して、Web セキュリティアプライアンス を Cisco Cloud Services ポータルに接続します。

ステップ 6 変更を送信し、保存します。

ステップ 7 数分待ってから、[登録（Register）] ボタンが [クラウドサービス設定（Cloud Services Settings）] ページに表示されるかどうかを確認します。

（注） CLI を使用して Cisco Cloud Services ポータルを有効にするには、`cloudserviceconfig` コマンドを使用します。

次のタスク

Cisco Cloud Services ポータルに Web セキュリティアプライアンス を登録します。詳細については、https://securex.us.security.cisco.com/settings/modules/available に移動して、Cisco SecureX 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。

Cisco Cloud Services ポータルへの Web セキュリティアプライアンス の登録

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 [クラウドサービス設定（Cloud Services Settings）] の下に、登録トークンを入力し、**[登録（Register）]** をクリックします。

（注） CLI を使用して Web セキュリティアプライアンス を Cisco Cloud Services ポータルに登録するには、`cloudserviceconfig` コマンドを使用します。

アプライアンスにスマートライセンスが登録されている場合は、Cisco Cloud サービスを無効化または登録解除できません。

Cisco SecureX Ribbon を使用した攻撃分析の実行

（注） AsyncOS 14.0 以前のバージョンからダウングレードする場合、**ケースブック**は Cisco SecureX Ribbon の一部となります。

Cisco SecureX は、可視性の統合、自動化の実現、インシデント対応ワークフローの迅速化、脅威ハンティングの改善を行う一連の分散型機能をサポートします。Cisco SecureX の分散機能は、SecureX リボンでアプリケーションおよびツールの形式で利用できます。

この章で説明する内容は、次のとおりです。

- Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （9 ページ）

Cisco SecureX Ribbon はページの下部ペインにあり、ダッシュボードと環境内の他のセキュリティ製品間を移動しても保持されます。Cisco SecureX Ribbon は、次のアイコンと要素で構成されています。

- [リボンの展開/縮小（Expand/Collapse Ribbon）]
- Home
- ケースブックアプリ
- Incidents アプリ
- Orbital アプリ
- [エンリッチメント（Enrichment）] 検索ボックス
- 観測対象の検索
- 設定

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon を参照してください。

Cisco SecureX Ribbon へのアクセス

始める前に

前提条件 （3 ページ）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。

（注） AsyncOS の以前のバージョンで**ケースブック**を設定していたものとします。次の手順で説明するように、追加のスコープを持つ Cisco SecureX API クライアントで新しい [クライアントID（Client ID）] と [クライアントのシークレット（Client Secret）] を作成する必要があります。

 ボタンを使用して、ページの下部ペインにある Cisco SecureX リボンを右からドラッグできます。

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、新しい Web インターフェイスの Web レポート ページの概要を参照してください。

ステップ 2 [Cisco SecureX Ribbon] をクリックします。

ステップ 3 **SecureX API クライアント**で[クライアントID（Client ID）]と[クライアントのシークレット（Client Secret）]を作成します。API クライアントのクレデンシャルを生成する方法の詳細については、「Creating an API Client」を参照してください。

クライアント ID とクライアントパスワードの作成時には、次の範囲を選択してください。

- casebook
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profile
- private-intel
- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (アクセス権がある場合)

ステップ 4 アプライアンスの **[SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）]** 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 [SecureXリボンを使用するにはログインしてください（Login to use SecureX Ribbon）] ダイアログボックスで必要な Cisco SecureX 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 SecureX サーバを編集する場合は、Cisco SecureX リボンを右クリックして詳細を追加します。

次のタスク

Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加 （9 ページ）

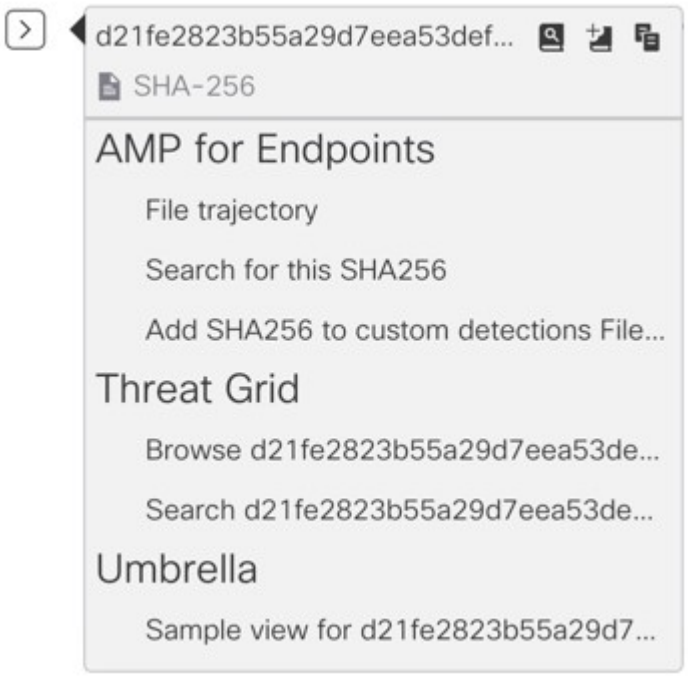
Cisco SecureX Ribbon およびピボットメニューを使用した攻撃分析のためのケースブックへの観察対象の追加

始める前に

アプライアンスの Cisco SecureX Ribbon 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、Cisco SecureX Ribbon へのアクセス （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、新しい Web インターフェイスの Web レポート ページの概要を参照してください。

ステップ 2 [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ます。



次の手順を実行します。

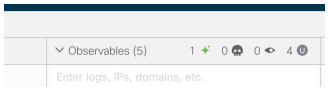
- アクティブなケースに観測対象を追加するには、 ボタンをクリックします。
- 新しいケースに観測対象を追加するには、 ボタンをクリックします。

（注） 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  アイコンにカーソルを合わせ、  ボタンをクリックして**ケースブック**を開きます。観測対象が新しいまたは既存のケースに追加されたかどうかを確認します。

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。

（注） 脅威分析の観測対象を検索するには、次の 2 つの方法があります。

- Cisco SecureX の[エンリッチメント（Enrichment）]  検索ボックスをクリックし、観測対象を検索します。
- Cisco SecureX Ribbon 内の [ケースブック（Casebook）] アイコンをクリックし、  フィールドで観測対象を検索します。

Cisco SecureX Ribbon の詳細については、https://securex.us.security.cisco.com/help/ribbon 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。