



Cisco Secure Cloud Analytics

Umbrella との統合クイックスタートガイド



目次

Cisco Secure Cloud Analytics と Umbrella との統合	3
Umbrella Investigate アクセストークンの生成	3
Umbrella Investigate アクセストークンの生成:	3
Secure Cloud Analytics への Umbrella アクセストークンのアップロード	4
Umbrella アクセストークンのアップロード:	4
Umbrella との統合の確認と使用	4
Secure Cloud Analytics Web ポータルでの Umbrella 情報の表示:	6
Umbrella を使用して IP アドレス情報に直接アクセスします。	6
関連リソース	7
サポートへの問い合わせ	8
変更履歴	9

Cisco Secure Cloud Analytics と Umbrella との統合

Cisco Secure Cloud Analytics (旧 Stealthwatch Cloud) を Umbrella Investigate REST API と統合することで、Secure Cloud Analytics Web ポータルで外部エンティティ IP アドレスに関する追加情報を提供できます。Umbrella によって生成される追加情報には、位置情報関連の情報、エンティティに対して検出されたドメイン名、および関連付けられた悪意のあるドメイン名が含まれます。Secure Cloud Analytics Web ポータルからクリックして Umbrella インターフェイスを新しいウィンドウで開き、エンティティに関する詳細情報を表示できます。

Secure Cloud Analytics を Umbrella と統合するには、Umbrella Investigate アクセストークンを生成して、Secure Cloud Analytics Web ポータルにアップロードします。この統合には、Secure Cloud Analytics の導入と Umbrella Investigate REST API のサブスクリプションが必要です。詳細については、<https://umbrella.cisco.com/products/packages> を参照してください。

Umbrella Investigate アクセストークンの生成

Umbrella Investigate REST API との通信を可能にするために、Umbrella Investigate アクセストークンを生成します。詳細については、<https://docs.umbrella.com/developer/investigate-api/about-the-api-authentication/> を参照してください。

Umbrella Investigate アクセストークンの生成:

はじめる前に

- Umbrella Investigate UI に管理者アカウントでログインします。

手順

1. [設定 (Settings)] アイコン > [APIアクセス (API Access)] を選択します。
2. [新しいトークンの作成 (create new token)] をクリックします。
3. **アクセストークン名**を入力します。
4. [作成 (Create)] をクリックします。

Secure Cloud Analytics への Umbrella アクセストークンのアップロード

Umbrella Investigate アクセストークンを生成したら、Secure Cloud Analytics Web ポータルにアップロードして Umbrella Investigate REST API との通信を有効にし、Umbrella から DNS をはじめとする情報を受信します。

Umbrella アクセストークンのアップロード:

はじめる前に

- Secure Cloud Analytics Web ポータルに管理者アカウントでログインします。


手順

1. [設定 (Settings)] > [統合 (Integrations)] > [Umbrella] を選択します。
2. [トークンの編集 (Edit Token)] をクリックしてセクションを展開します。
3. Umbrella アクセストークンをコピーして、[新しいアクセストークン (New Access Token)] フィールドに貼り付けます。
4. [有効 (Enabled)] を選択します。
5. [保存 (Save)] をクリックします。

Umbrella との統合の確認と使用

Secure Cloud Analytics と Umbrella の統合が完了したら、外部 IP アドレスにカーソルを合わせると、外部 IP アドレスの Umbrella DNS 関連情報を Web ポータルから直接表示できます。これには、検出された組織に関連付けられているホスティング組織、地理位置情報、およびその他の悪意のあるドメイン名に関する情報が含まれます。

Umbrella UI に直接アクセスして、IP アドレスに関する追加情報を表示することもできます。

 Secure Cloud Analytics で Umbrella DNS 関連情報の表示が開始されるまで、最大 10 分かかります。この情報が表示されない場合は、[シスコサポート](#)までお問い合わせください。

次に、Umbrella と Secure Cloud Analytics を統合した場合に Secure Cloud Analytics Web ポータルに表示される可能性のあるフィールド情報について説明します。

Umbrella 統合フィールド

フィールド	説明	書式
ASN CIDR	Umbrella によって識別された、この IP アドレスが属する組織に関連付けられた CIDR 範囲。 これには、IP アドレスに関する追加情報の Umbrella へのリンクが含まれています。	CIDR 範囲。
ASN Description	Umbrella によって識別された、この IP アドレスが属する組織名。	組織名
ASN Region	Umbrella によって識別された、この IP アドレスの発信元地域のインターネットレジストリ。	次の地域インターネットレジストリのいずれか： <ul style="list-style-type: none"> • APNIC – アジア太平洋ネットワーク情報センター • RIPE NCC – ヨーロッパ IP リソースネットワーク調整センター • AFRINIC – アフリカのネットワーク情報センター • ARIN – American Registry for Internet Numbers • LACNIC – 中南米およびカリブネットワーク情報センター
Country	Umbrella によって識別された、この IP アドレスの発信元の国。表示される地理位置情報フラグアイコンと一致します。	国名。
DNS Name	Umbrella によって識別された、このエンティティのドメイン名。	ドメイン名。
Umbrella	Umbrella によって識別された、この組織がホストしたことのある悪意のあるドメインの数。 これには、IP アドレスに関する追加情報の Umbrella へのリンクが含まれています。	悪意のあるドメインの数。

Secure Cloud Analytics Web ポータルでの Umbrella 情報の表示:

はじめる前に

- Secure Cloud Analytics Web ポータルに管理者アカウントでログインします。

手順

- 外部 IP アドレスの場合は、ポインタを位置情報アイコンの上に置きます。

Umbrella を使用して IP アドレス情報に直接アクセスします。

はじめる前に

- Secure Cloud Analytics Web ポータルに管理者アカウントでログインします。

手順

- 次の選択肢があります。
 - 外部 IP アドレスの場合、ポインタを位置情報アイコンの上に置き、[詳細 (details)] をクリックします。
 - 外部 IP アドレスの場合、IP アドレスをクリックしてから、[Cisco Umbrella] をクリックします。

関連リソース

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、<https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> を参照してください。
- 60 日間の無料トライアルに登録するには、<https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> にアクセスしてください。
- ドキュメントリソースについては、<https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> を参照してください。
- Secure Cloud Analytics 初期導入ガイドなど、インストールおよびコンフィギュレーション ガイドについては、<https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> を参照してください。

サポートへの問い合わせ

テクニカルサポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコパートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：<http://www.cisco.com/c/en/us/support/index.html>
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447(米国)
- ワールドワイド サポート番号：
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>
- Secure Cloud Analytics 無料トライアルの試用時に電子メールでケースを開く場合：
swatchc-support@cisco.com

変更履歴

リビジョン	改訂日	説明
1.0	2019年1月16日	最初のバージョン。
1.1	2020年10月16日	UIの更新に基づく更新。
2.0	2021年11月3日	製品のブランド名を更新。
2.1	2022年8月4日	「サポートへの問い合わせ」セクションを追加。

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)