Cisco Secure Cloud Analytics コネクタの設定

Cisco Connector for Secure Cloud Analytics の設定

Cisco Secure Cloud Analytics（旧称 Stealthwatch Cloud）は、悪意のある各種アクティビティをリアルタイムで特定するために必要な、実用的なセキュリティインテリジェンスと可視性を提供します。セキュリティインシデントが壊滅的な侵害になる前に迅速に対応できます。このガイドでは、シスコ産業用イーサネットスイッチでの IOS-XE での Cisco Cloud Connector の設定手順について説明します。

（注） Cisco Secure Cloud Analytics（Stealthwatch Cloud）または Cisco Secure Network Analytics（Stealthwatch）の詳細については、次の URL を参照してください。https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

制限事項と制約事項

- 事前に定義された一連のフィールドのみを収集できます。対象のフィールドには、送信元 IP、送信元ポート、宛先 IP、宛先ポートおよびプロトコルの 9 タプルフローデータと、フロー開始、フロー終了、パケット数、およびバイト数が含まれます。
- 必須フィールドは、CLI の制限では適用されません。レコードにすべての必須フィールドがなく、9 タプルデータを収集できない場合、そのフローは破棄されます。
- Cisco Secure Cloud Analytics 用の StealthWatch コネクタは、スイッチのルーティング機能を使用して、クラウドサーバにパケットを送信します。追加のチェックは行われません。適切なルートが存在することを前提としています。

- モニタアプリケーションの観点から Flexible NetFlow 固有のモニタアプリケーションの制限は、Cisco Secure Cloud Analytics にも当てはまります。例：SVI なし、VLAN なし、送信モニタなし。
- クラウドエクスポータを他のエクスポータと一緒に使用することはできません。
- アップロードされたファイルの命名規則には、すべてのファイルを一意に識別し、ファイルの上書きを防ぐためのランダムな文字列が含まれています。例：https://sensor.ext.obsrvbl.com/sign/ios-xe-17-2/2019/7/5/00:00:00/hostname-random_suffix.csv.gz。1 分ごとに集約されてアップロードされます。

始める前に

Cisco Secure Cloud Analytics コネクタは、IE3300、IE3400、IE3400H スイッチでのみサポートされます。

- Network Advantage および Cisco DNA Advantage ライセンス

手順の概要

1. stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
2. フローレコード SWCRec
3. フローエクスポータ SWCExp
4. インターフェイス gi1/0/3

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
	例：
	`stealthwatch-cloud-monitor`
	`  service-key <you service key>`
	`  hostname my_sensor`
	`  url https://sensor.ext.obsrvbl.com`
	`openssl s_client -showcerts -connect`
	`https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect`
	`s3.ap-southeast-2.amazonaws.com:443`
	例：
	`openssl s_client -showcerts -connect`
	`https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect`
	`s3.ap-southeast-2.amazonaws.com:443`
		URL に基づいて有効なルート CA をインストールしてください。以下の CLI を使用して、URL に従ってルート CA を把握してください
		センサーの登録に使用されるサービスキーとホスト名を設定します。ホスト名を指定しない場合は、ボックスのシリアル番号が登録に使用されます。

ステップ 2	フローレコード SWCRec
	例：
	`flow record SWCRec`
	`match ipv4 source address`
		Cisco Secure Cloud Analytics レコードのデータを収集するためのフローレコードのフィールドを設定します。

	コマンドまたはアクション	目的
	match ipv4 destination address match transport source-port match transport destination-port match ipv4 protocol collect counter bytes long collect counter packets long collect timestamp sys first collect timestamp sys last	
ステップ 3	フローエクスポータ SWCExp **例：** flow exporter SWCExp destination stealthwatch-cloud flow monitor SWCMon flow record SWCRec flow exporter SWCExp	Cisco Secure Cloud Analytics エクスポータを設定し、フローモニタに接続して、Secure Cloud へのエクスポートを開始します。
ステップ 4	インターフェイス gi1/0/3 **例：** Interface gi1/0/3 ip flow monitor SWCMon input	フローをモニタするインターフェイスを特定し、Cisco Secure Cloud Analytics エクスポータがあるモニタをそのインターフェイスに接続します。

次のタスク

Cisco Secure Cloud Analytics の詳細情報については、該当するコンフィギュレーション ガイドを参照してください。https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-and-configuration-guides-list.html

トラブルシューティング

- デバッグログは「debug Stealthwatch」CLI を使用して有効にできます。

```
switch#debug stealthwatch-cloud ?
  all          All debugs for SWC
  cert         Certificate Validation
  error        errors
  event        Events
  file-events  File notifications
```

- プラットフォームレベルのデバッグでは、「debug platform software swc」CLI を使用できます。

```
switch#debug platform software swc ?
  all         all
  errors      Stealthwatch Cloud errors
  events      Stealthwatch Cloud events
  pkt-events  Stealthwatch Cloud data collection events
```

コマンドの表示

- **Switch-1# show stealthwatch-cloud detail**

```
=======================================
Stealthwatch Cloud Parameters
=======================================
   Service Key  : x8SS2q7e4twpcNWT35AsL6i6xHd24iXJvICo3N4sGx1U1pCqqs
   Sensor Name  : petra
   URL          : https://sensor.anz-prod.obsrvbl.com
=======================================
Stealthwatch Cloud Sensor Info
=======================================
   Sensor Status    : Registered
   Last heartbeat   : 2020-05-08T12:11:50
```

- **Switch-1# show platform software swc stats**

```
=========================
SWC Upload Statistics:
=========================
1 : Last file uploaded          :  202005081212_ufihi2
2 : Time of upload              :  202005081213 UTC
3 : Current file uploading      :
4 : Files queued for upload     :
5 : Number of files queued      :  0
6 : Last failed upload          :
7 : Files failed to upload      :  0
8 : Files successfully uploaded :  416
=========================
SWC File Creation Statistics:
=========================
9 : Last file created           :  202005081212_ufihi2
10: Time of creation            :  202005081212 UTC
=========================
SWC Flow Statistics:
=========================
11: Number of flows in prev file:  1
12: Number of flows in curr file:  0
13: Invalid dropped flows       :  0
=========================
SWC Flags:
=========================
14: Is Registered               :  Registered
15: File Delete         :  Enabled
16: Exporter            :  Enabled
```