STIX/TAXII サービス

- 新機能 （1 ページ）
- 概要 （1 ページ）
- ポーリングサービス （2 ページ）
- 共通のクエリ （11 ページ）
- Cisco ISE との統合 （13 ページ）

新機能

2022 年後半に、グローバル脅威アラートは STIX/TAXII API のサポートを停止します。

代わりに、新しい REST API（2021 年 6 月に導入）を使用することをお勧めします。

- アクセスするには、https://api.cta.eu.amp.cisco.com のドキュメントに従ってください。
- 詳細については、「グローバル脅威アラートの REST API がリリースされました」を参照してください。
- サポートが必要な場合は、cognitive-api-support@cisco.com までお問い合わせください。

概要

グローバル脅威アラートでは、詳細な相関分析およびアーカイブのために、検出されたインシデントの情報をクライアントに取り込むことができます。これを使用して、すべてのアラートをネットワーク内のサードパーティ SIEM にストリーミングすることで、データ収集プロセス全体を自動化したりすることもできます。このサービスは、Security Information and Event Management（SIEM）システムとの統合のため、MITRE の Trusted Automated eXchange of Indicator Information（TAXII）標準をサポートしています。TAXII 標準は、システム間のサイバー脅威情報の共有に使用される転送メカニズムを指定するものです。

TAXII の詳細については、次を参照してください。

TAXII MITRE 組織

TAXII プロジェクト GitHub

各インシデントの情報は、Structured Threat Information eXpression（STIX）言語形式を使用して表されます。STIX はサイバー脅威情報を表す構造化言語であるため、一貫した方法で共有、保存、および分析できます。STIX 形式を使用すると、グローバル脅威アラートでは、階層形式で侵害検出の調査結果を表示できます。TAXII サービスは、グローバル脅威アラートが検出したインシデントの記述に STIX 言語のサブセットを使用します。現在サポートされているオブジェクトは次のとおりです。

- キャンペーン - 確認された脅威カテゴリ（利用できる場合）
- インシデント - 異常な活動
- TTP - 戦術、手法、手段
- 監視 - Web 要求
- インジケータ - 観察可能な条件を識別するパターン

STIX の詳細については、次を参照してください。

https://stix.mitre.org/

ポーリングサービス

ポーリングサービスは、標準化された TAXII 転送メカニズムを使用してグローバル脅威アラートから TAXII 規格をサポートするクライアントにインシデント情報を送信します。インシデント情報を取得するには、TAXII クライアントは TAXII ポーリングサービスにポーリング要求を送信します。承認されたユーザだけにアクセスを制限するため、HTTP 基本認証が使用されます。次に、TAXII ポーリングサービスは、グローバル脅威アラートから TAXII クライアントにインシデント情報を送信することで応答します。すべてのデータ転送を保護するために HTTPS プロトコルが使用されます。

SIEM やその他のセキュリティ ワークフロー システムは、ネイティブで STIX/TAXII をサポートしている必要があります。サードパーティの TAXII クライアントが定期的に TAXII ポーリングサービスにポーリングを実行するように構成します。

- アカウント情報を取得するには、STIX/TAXII サービスを要求します。
  1. 右上隅にあるグローバル設定の歯車アイコンをクリックします。
  2. [CTA STIX/TAXII API] をクリックします。
  3. [Add account] ボタンをクリックします。
  4. アカウントを特定する名前を入力し、[Add account] ボタンをクリックします。
- プロビジョニングプロセスが完了したら、アカウント情報が表示されます。ウィンドウを閉じる前に、安全な場所にこのアカウント情報をコピーします。

（注） セキュリティ上の理由により、シークレットパスワードは 1 度しか表示されません。シークレットパスワードを失くした場合は、既存のシークレットパスワードを廃止し、新しいシークレットパスワードを生成する必要があります。

- 固有の属性をサードパーティの TAXII クライアントにコピーするには、次のものを使用します。
  - pollEndpoint またはフィードサービス URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
  - username
  - password
  - コレクション名またはフィード名

（注） Cognitive Intelligence（旧 Cognitive Threat Analytics または CTA）は、2018 年 8 月に Amazon Web Services の新しい場所への移行を開始したため、サービスにアクセスして使用するための新しい IP アドレスと追加の URL があります。サービスへのアクセスを維持するには、アウトバウンド ファイアウォール ルールの更新が必要な場合があります。2018 年 11 月のスイッチオーバー後は、古いデータ取得サービスの IP アドレスにデータを正常に送信できなくなります。必要な変更およびその他の重要な情報の詳細については、「Field Notice」を参照してください。

（注） シスコでは、サードパーティ製品または SIEM デバイスを構成するためのテクニカルサポートを提供していません。問題発生時には、ベンダー固有のサポートチームに問い合わせてください。

または、シスコから TAXII クライアント例をダウンロードして使用できます。SIEM または他のセキュリティシステムがネイティブで STIX/TAXII をサポートしていない場合、シスコは軽量な Java TAXII Log Adapter を提供します。これは、SIEM の最も近くにある Linux または Windows の仮想マシン環境に配備できます。セットアップ手順を表示するために提供されているリンクをクリックします。アダプタは、TAXII API を使用して、新しいインテリジェンスの定期的ポーリングを実行し、データを STIX メッセージで提供します。STIX メッセージは、アダプタによって、一般的な SIEM システムで受け入れられる他の形式に変換されます。

ポーリングサービスの安定性、パフォーマンス、および可用性をサポートするには、次を行います。

- 1 つの TAXII クライアントに許容されるポーリングは、10 分ごとに 1 回だけです。それ以外の場合、このエラーを示すステータスメッセージが返されます。

- ポーリング要求は、最大で 3 日までインシデント情報を取得できます。
- インシデント情報は、30 日間取得できるように保存されます。

ポーリング要求

TAXII クライアントから TAXII ポーリングサービスへのポーリング要求の例を次に示します。

メソッドは POST です。

HTTP 要求ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

要求本文：

```
<taxii_11:Poll_Request
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                            message_id=" " collection_name=" ">

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

サポートされる要求パラメータ	説明
Poll_Request	
message_id	TAXII 仕様に従って、各要求に対してランダムに生成された文字列。要求ごとに一意の文字列を再生成します。
collection_name	グローバル脅威アラートサービスから抽出または取得されるコレクションの名前。この属性は、Cisco によってプロビジョニングプロセスの完了後に提供されます。
Exclusive_Begin_Timestamp	時間枠に応じてこの値を調整します。
Inclusive_End_Timestamp	時間枠に応じてこの値を調整します。
Poll_Parameters	

サポートされる要求パラメータ	説明
allow_asynch	この属性は常に false に設定します。

（注） **Exclusive_Begin_Timestamp** と **Inclusive_End_Timestamp** の間でサポートされる最大の差は 3 日です。差がこれを超えている場合、返される結果は **Inclusive_End_Timestamp** から 3 日前までに制限されます。

ポーリング応答

TAXII ポーリングサービスから TAXII クライアントへのポーリング応答の例を次に示します。

HTTP 応答ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

応答本文：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Poll_Response xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                 xmlns:c="http://cybox.mitre.org/cybox-2"
                 xmlns:cc="http://cybox.mitre.org/common-2"
                 xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
                 xmlns:coa="http://stix.mitre.org/CourseOfAction-1"
                 xmlns:sc="http://stix.mitre.org/common-1"
                 xmlns:ind="http://stix.mitre.org/Indicator-2"
                 xmlns:ttp="http://stix.mitre.org/TTP-1"
                 xmlns:inc="http://stix.mitre.org/Incident-1"
                 xmlns:s="http://stix.mitre.org/stix-1"
                 collection_name=" " more="true"
                  result_id=" " result_part_number="1"
                  in_response_to="generatedMessageID" message_id="responseMessageID">
    <t:Exclusive_Begin_Timestamp>2015-01-17T15:11:00.648Z</t:Exclusive_Begin_Timestamp>
    <t:Inclusive_End_Timestamp>2015-01-20T15:11:00.649Z</t:Inclusive_End_Timestamp>
    <t:Content_Block>
      <t:Content_Binding binding_id="STIX_XML_1.1"/>
      <t:Content>
        <s:STIX_Package xmlns:cta="http://cisco.com/td/cta"
                id="cta:package-1412045744-66911c07-c9b8-4389-8888-00e438f58c2e"
                timestamp="2015-01-20T15:11:02.766Z" version="1.1.1">
          <s:STIX_Header>
            <s:Package_Intent>Incident</s:Package_Intent>
              <s:Information_Source>
                <sc:Identity id="cta:customer-1234567890"/>
                <sc:Tools>
                   <cc:Tool id="cta:tool-cta">
                       <cc:Name>Cognitive Threat Analytics</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
                   <cc:Tool id="cta:tool-amp">
                       <cc:Name>Advanced Malware Protection</cc:Name>
                       <cc:Vendor>Cisco</cc:Vendor>
                   </cc:Tool>
```

```
                    </sc:Tools>
                  </s:Information_Source>
                </s:STIX_Header>
                <s:Incidents>
                  <s:Incident xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                          xsi:type="inc:IncidentType"
                          id="cta:incident-1412045744_f8bae03fb2ff7d6185907ae3240d_ITMAL1">
                   <inc:Title>malware|using automatically generated domain (DGA)</inc:Title>
                   <inc:Victim>
                       <sc:Name>JohnDoe</sc:Name>
                   </inc:Victim>
                    <inc:Related_Indicators>
                     <inc:Related_Indicator>
                      <sc:Indicator xsi:type="ind:IndicatorType"

id="cta:indicator-1412045744_1421623800000_f8bae03fb2ff7d6185907ae3240d_0">
                       <ind:Observable>
                        <c:Observable_Composition operator="AND">
                          <c:Observable>
                           <c:Object>
                            <c:Properties xsi:type="co:CustomObjectType">
                             <cc:Custom_Properties>
                              <cc:Property name="timestamp">1421623882432</cc:Property>
                              <cc:Property name="xElapsedTime">1810</cc:Property>
                              <cc:Property name="scHttpStatus">0</cc:Property>
                              <cc:Property name="csContentBytes">622</cc:Property>
                              <cc:Property name="scContentBytes">907</cc:Property>
                              <cc:Property name="csUrl"></cc:Property>
                              <cc:Property name="sIP">195.22.26.231</cc:Property>
                              <cc:Property name="cIP">33.196.39.11</cc:Property>
                              <cc:Property name="cUsername">JohnDoe</cc:Property>
                              <cc:Property name="sReputation">-580</cc:Property>
                              <cc:Property name="sCategory">unclassified</cc:Property>
                             </cc:Custom_Properties>
                            </c:Properties>
                           </c:Object>
                          </c:Observable>
                          <c:Observable>
                           <c:Object>
                            <c:Properties xsi:type="co:CustomObjectType">
                             <cc:Custom_Properties>
                              <cc:Property name="timestamp">1421623896635</cc:Property>
                              <cc:Property name="xElapsedTime">1942</cc:Property>
                              <cc:Property name="scHttpStatus">0</cc:Property>
                              <cc:Property name="csContentBytes">361</cc:Property>
                              <cc:Property name="scContentBytes">582</cc:Property>
                              <cc:Property name="csUrl"></cc:Property>
                              <cc:Property name="sIP">195.22.26.231</cc:Property>
                              <cc:Property name="cIP">33.196.39.11</cc:Property>
                              <cc:Property name="cUsername">JohnDoe</cc:Property>
                              <cc:Property name="sReputation">-580</cc:Property>
                              <cc:Property name="sCategory">unclassified</cc:Property>
                             </cc:Custom_Properties>
                            </c:Properties>
                           </c:Object>
                          </c:Observable>
                         </c:Observable_Composition>
                        </ind:Observable>
                        <ind:Indicated_TTP>
                         <sc:TTP xsi:type="ttp:TTPType">
                          <ttp:Title>communication to automatically generated domain
(DGA)</ttp:Title>
                         </sc:TTP>
                        </ind:Indicated_TTP>
```

```
                    </sc:Indicator>
                   </inc:Related_Indicator>
                  </inc:Related_Indicators>
                  <inc:Discovery_Method>Log Review</inc:Discovery_Method>
                  <inc:COA_Requested>
                   <inc:Course_Of_Actionxsi:type="coa:CourseOfActionType">
                    <coa:Stage>Remedy</coa:Stage>
                    <coa:Type>Eradication</coa:Type>
                  <coa:Parameter_Observablescybox_major_version="2"cybox_minor_version="1">

                     <c:Observable_Package_Source>
                      <cc:Time>
                       <cc:Produced_Time>2016-08-15T17:02:02.616Z</cc:Produced_Time>
                      </cc:Time>
                     </c:Observable_Package_Source>
                     <c:Observable>
                      <c:Object>
                       <c:Propertiesxsi:type="user:UserAccountObjectType">
                        <user:Username>JohnDoe</user:Username>
                       </c:Properties>
                      </c:Object>
                     </c:Observable>
                     <c:Observable>
                      <c:Object>
                       <c:Propertiesxsi:type="addr:AddressObjectType"category="ipv4-addr">
                        <addr:Address_Value>33.196.39.11</addr:Address_Value>
                       </c:Properties>
                      </c:Object>
                     </c:Observable>
                    </coa:Parameter_Observables>
                   </inc:Course_Of_Action>
                  </inc:COA_Requested>
                  <inc:Confidence>
                   <sc:Value>Low</sc:Value>
                  </inc:Confidence>
                  <inc:Information_Source>
                      <sc:Tools>
                          <cc:Tool idref="cta:tool-cta"/>
                      </sc:Tools>
                  </inc:Information_Source>
              </s:Incident>
             </s:Incidents>
            </s:STIX_Package>
           </t:Content>
      </t:Content_Block>
</t:Poll_Response>
```

（注） `Poll_Reponse` では、これ以上脅威項目がない場合、`more` と `result_id` の 2 つの属性はありません。`more=true` が指定されている場合は、`Poll_Fulfillment` を使用して応答の次のページを要求できます。

サポートされる応答オブジェクト	フィールドの説明
Poll_Response	

サポートされる応答オブジェクト	フィールドの説明
collection_name	グローバル脅威アラートサービスから抽出または取得されるコレクションの名前。この属性は、Ciscoによってプロビジョニングプロセスの完了後に提供されます。
result_id	この値をポーリング履行要求にコピーします。
Exclusive_Begin_Timestamp	このポーリング応答によって対応する時間範囲の最初（この値を含まない）。このフィールドがない場合は、ポーリング応答がこのTAXIIデータフィードの最も早い時間に対応することを示します。
Inclusive_End_Timestamp	このポーリング応答によって対応する時間範囲の最後（この値を含む）。
Content_Block	返されたコンテンツ。
Content_Binding	
Content	
STIX_Package	STIX言語に関する情報。
STIX_Header	STIXコンテンツのこのパッケージに関する情報。
Incidents	1つ以上のインシデント。
Incident	1つのインシデントに関する情報。
Title	このインシデントを説明するタイトル。
Victim	このインシデントの被害者に関する情報。
Related_Indicators	このインシデントに関連するインジケータを識別します。
Related_Indicator	このインシデントに関連する1つのインジケータを識別します。
Indicator	特定の観察可能な条件を識別するパターン、パターンの意味に関するコンテキスト情報、パターンのアクションの方法およびタイミングなどで構成されるインジケータ。
Observable	このインジケータに関連する監視。

サポートされる応答オブジェクト	フィールドの説明
Observable_Composition	他の監視の論理的な組み合わせを作成することで、高次の複合監視を指定できます。
Observable	単一の監視を表します。
Object	特定のオブジェクト（ファイル、レジストリキー、プロセス）の特性を識別します。
Properties	オブジェクトの操作の結果として列挙されたプロパティ。
Custom_Properties	既存の Properties スキーマで定義できない一連のカスタムオブジェクトのプロパティを指定することができます。
Property	オブジェクトの操作の結果として列挙された単一のプロパティ。
Indicated_TTP	このインジケータが示す、関連する戦術、手法、手段（TTP）を指定します。
Discovery_Method	コードを検出するために使用される手法やツールに関する情報。
COA_Requested	このインシデントに推奨される一連のアクション。
Confidence	このインシデントの特性で保持されている信頼性のレベルに関する情報。
Information_Source	このインシデントのソースに関する情報。
Tools	
Tool	CTA と AMP のどちらのツールが、このインシデントを検出したか。

エラーが発生した場合、エラー メッセージが返されます。次に例を示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<t:Status_Message
          xmlns:t="http://taxii.mitre.org/messages/taxii_xml_binding-1"
          xmlns:c="http://cybox.mitre.org/cybox-2"
          xmlns:cc="http://cybox.mitre.org/common-2"
          xmlns:co="http://cybox.mitre.org/objects#CustomObject-1"
          xmlns:sc="http://stix.mitre.org/common-1"
          xmlns:ind="http://stix.mitre.org/Indicator-2"
          xmlns:ttp="http://stix.mitre.org/TTP-1"
          xmlns:inc="http://stix.mitre.org/Incident-1"
          xmlns:s="http://stix.mitre.org/stix-1"
                status_type="FAILURE" in_response_to="23537"
```

```
                message_id="16ed0b75-2af6-4537-b71c-da00e0a0c419">
   <t:Message>An error occurred during request processing.</t:Message>
</t:Status_Message>
```

TAXII status_type	エラーの説明
	ユーザは認証されておらず、HTTP 応答ステータスコードが 404 です。
DENIED	ユーザは認証されておらず、HTTP 応答ステータスコードが 401 です。
BAD_MESSAGE	無効な要求メッセージです。Message パラメータを参照してください。
FAILURE	未指定のエラーです。Message パラメータを参照してください。

ポーリング履行

TAXII クライアントから TAXII ポーリングサービスへのポーリング履行要求の例を次に示します。

メソッドは POST です。

HTTP 要求ヘッダー：

```
x-taxii-content-type: urn:taxii.mitre.org:message:xml:1.1
x-taxii-protocol: urn:taxii.mitre.org:protocol:http:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
x-taxii-accept: urn:taxii.mitre.org:message:xml:1.1
content-type: application/xml
accept: application/xml
authorization: Basic ...
```

要求本文：

```
<taxii_11:Poll_Fulfillment
xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1"
                           message_id=" " collection_name=" "
                           result_id=" " result_part_number="2" />

<taxii_11:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_11:Exclusive_Begin_Timestamp>


<taxii_11:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_11:Inclusive_End_Timestamp>

 <taxii_11:Poll_Parameters allow_asynch="false"/>
  <taxii_11:Response_Type>FULL</taxii_11:Response_Type>
 </taxii_11:Poll_Parameters>
</taxii_11:Poll_Request>
```

サポートされる要求パラメータ	説明
Poll_Request	
message_id	TAXII 仕様に従って、各要求に対してランダムに生成された文字列。要求ごとに一意の文字列を再生成します。
collection_name	グローバル脅威アラートサービスから抽出または取得されるコレクションの名前。この属性は、Cisco によってプロビジョニングプロセスの完了後に提供されます。
result_id	ポーリング応答からこの値を貼り付けます。
result_part_number	ポーリング応答の値からこの値を 1 増やします。
Exclusive_Begin_Timestamp	時間枠に応じてこの値を調整します。
Inclusive_End_Timestamp	時間枠に応じてこの値を調整します。
Poll_Parameters	
allow_asynch	この属性は常に false に設定します。

（注） **Exclusive_Begin_Timestamp** と **Inclusive_End_Timestamp** の間でサポートされる最大の差は 3 日です。差がこれを超えている場合、返される結果は **Inclusive_End_Timestamp** から 3 日前までに制限されます。

共通のクエリ

このセクションでは、詳細な調査に向けて結果に優先度を設定するため、Cisco STIX/TAXII API で使用される共通のクエリの一部について説明します。クエリ例で使用する構文は、SPLUNK の統合に基づいており、象徴的なものです。特定のフィールドや値はローカルの統合によって異なる可能性がありますが、クエリの意味は SIEM システムおよび統合に広く適用されます。

ヒント SPLUNK に他のデータを収集している場合、グローバル脅威アラートデータのみを介して検索するには、ホスト、インデックス、または送信元名の先頭にクエリを追加します。

Users Affected by Confirmed Threats

このクエリは確認済みの脅威を持つすべてのユーザを返します。また、デスクトップ修復のための Incident Response Team に報告することができます。これらのインシデントもリスクが高い場合は、影響を受けるデバイスの再イメージングを検討します。このクエリは、影響を受けるユーザ名およびキャンペーン名を持つテーブルを作成します。次のようにして空でないキャンペーン名を検索し、username+campaign ペアの重複を排除します。

```
campaign!="" | table cUsername campaign | dedup cUsername campaign | sort + cUsername
```

または、次のようにキャンペーン名の複数値のフィールドを使用します。

```
campaign!="" | transaction cUsername | table cUsername campaign | sort + cUsername
```

Users Affected by Confirmed Threats Within a Timeframe

このクエリには、最初に表示された列および最後に表示された列も含まれています。空でないキャンペーンを検索し、username+campaign ペアで集約し、Web フローのタイムスタンプの最小値および最大値を計算します。結果はエポックミリ秒単位ですが、必要に応じて、カレンダー時間に変換できます。

```
campaign!="" | stats min(timestamp) max(timestamp) by cUsername campaign
```

または、strftime 関数を使用してエポックの変換を含めます。次の例では、ミリ秒を削除するため、タイムスタンプを 1000 で割っています。

```
campaign!="" | stats min(timestamp) as oldest max(timestamp) as newest by cUsername
campaign |
  eval oldest_time=strftime(oldest/1000,"%m/%d/%y %H:%M:%S") |
  eval newest_time=strftime(newest/1000,"%m/%d/%y %H:%M:%S") |
  table cUsername, campaign, oldest_time, newest_time
```

Users Affected by High Risk and High Confidence Incidents

このクエリは、確認されたキャンペーンの有無にかかわらず、高いリスクおよび高い信頼性を持つユーザの優先順位リストのテーブルを生成します。高いリスクと高い信頼性を検索し、ユーザ名の重複を排除します。これらすべてのインシデントは高いリスクかつ高い信頼性であるため、影響を受けるデバイスの再イメージングを検討します。

```
confidence="High" risk="High" | dedup cUsername | table cUsername campaign
```

Users Affected by Campaign

このクエリは、感染したユーザ数について、時間の経過とともにキャンペーンで分割したグラフを生成します。空でないキャンペーンを検索し、1 日の期間で bin を実行し、その bin 内のユーザ名の明確な数を計算します。

```
campaign!="" | timechart dc(cUsername) span=1d by campaign
```

（注） SPLUNK では、タイム チャート ショートカットを使用できます。

コマンド アンド コントロール サーバー

このクエリは、確認されたカテゴリで検出されたすべてのコマンドおよび制御（C&C）サーバのリストを生成します。サーバのIPアドレスとキャンペーンを表示する一方で、空でないキャンペーンを探して、サーバ IP アドレスの重複を排除します。検索の結果、C&C の通信を維持するために感染したデバイスで使用される C&C 宛先 IP アドレスをリストします。各 C&C IP アドレスごとに、どの脅威キャンペーンに含まれているのかも分かります。より多くのインテリジェンスの他のシステムを照会し、セキュリティ侵害の指標（IOC）を提供し、感染したエンドポイントの悪意のあるプロセスとアプリケーションを特定するために使用できます。

```
campaign!="" | table sIP campaign | dedup sIP
```

Cisco ISE との統合

Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。Cisco ISE はポリシー デシジョン ポイントとして動作し、企業におけるコンプライアンスの遵守、インフラストラクチャのセキュリティの向上、およびサービス オペレーションの合理化を可能にします。企業は、Cisco ISE を使用して、ネットワーク、ユーザ、およびデバイスから状況情報をリアルタイムで収集できます。その後、その情報を使用して、ネットワーク内のさまざまな要素にアイデンティティを関連付けることで、プロアクティブなガバナンスの判断を行うことができます。

グローバル脅威アラートは Cisco ISE と統合され、ネットワークレベルの検疫を提供します。この機能は、感染したデバイスをネットワークから切断する機能を備えており、機密データをそれ以上漏洩できないようになっています。グローバル脅威アラートと Cisco ISE の統合では、STIX/TAXII を使用します。システムが個々のユーザに感染したと見なすことができる重大レベルのリスクが検出された場合、Cisco ISE は Requested Course of Action（要求された一連のアクション）を受信します。これにより Cisco Rapid Threat Containment フレームワークの一部である Threat Centric Network Access Control（TC-NAC）検疫が提案されます。Requested Course of Action は、感染に関連するリスクに応じて、モニタリング、根絶、内部ブロック、またはその組み合わせになります。内部ブロッキングは、TC-NAC のブロッキングポリシーで使用することを目的とした一連のアクションです。詳細については「Cisco Rapid Threat Containment」を参照してください。

Cisco ISE と、グローバル脅威アラート STIX/TAXII サービスによって提供されるデータフィードを使用して、独自のソリューションを開発できます。データフィードには、感染したデバイスの識別と実行するアクションに関する情報が含まれています。グローバル脅威アラート STIX/TAXII フィードの推奨事項に基づいて、Cisco ISE で検疫ポリシーを定義できます。Cisco ISE でグローバル脅威アラート アダプタを設定する方法については、『Cisco ISE Administrator Guide, Release 2.2』を参照してください。

（注） グローバル脅威アラートは Web プロキシログにクライアント IP またはユーザ名としてリストされているユーザ ID を処理します。具体的には、IP アドレスの場合、プロキシログで使用可能な IP アドレスが、企業内部ネットワークの（別のデバイスの）IP アドレスと競合する IP アドレスである可能性があります。たとえば AnyConnect 経由で接続するローミングユーザと、インターネットに直接接続するスプリットトンネルが自宅で獲得するローカル IP アドレス（例：10.0.0.x）が、企業内部ネットワークで使用されている重複するプライベート範囲の IP アドレスと競合することがあります。Rapid Threat Containment ポリシーを定義する場合は、不適合デバイスに検疫アクションが適用されないように、論理ネットワークアーキテクチャを考慮してください。

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。