STIX/TAXII 서비스

새로운 기능

2022년 하반기부터는 전역 위협 알림이 STIX/TAXII API를 지원하지 않습니다.

(2021년 6월에 도입된) 새 REST API를 대신 사용하는 것이 좋습니다.

- 이 API에 액세스하려면 https://api.cta.eu.amp.cisco.com에 있는 설명서를 따르십시오.
- 자세한 내용은 전역 위협 알림 REST API가 릴리스되었습니다!를 참조하십시오.
- 도움이 필요하다면 cognitive-api-support@cisco.com으로 문의하십시오.

개요

전역 위협 알림을 사용하면 추가 상관관계 분석 및 보관을 위해 탐지된 인시던트에 관한 정보를 클라이언트로 가져올 수 있습니다. 모든 알림을 네트워크의 서드파티 SIEM으로 스트리밍하여 전체 데이터 수집 프로세스를 자동화할 수도 있습니다. 이 서비스는 보안 정보 및 이벤트 관리(SIEM) 시스템과의 통합을 위한 MITRE의 TAXII(Trusted Automated eXchange of Indicator Information) 표준을 지원합니다. TAXII 표준은 시스템 간에 사이버 위협 정보를 공유하는 데 사용하는 전송 메커니즘을 지정합니다.

TAXII에 대한 자세한 내용은 다음을 참조하십시오.

TAXII MITRE 조직

TAXII 프로젝트 GitHub

각 인시던트의 정보는 STIX(Structured Threat Information eXpression) 언어 형식으로 표시됩니다. STIX는 일관된 방식으로 공유, 저장 및 분석할 수 있도록 사이버 위협 정보를 설명하는 데 사용하는 구조적 언어입니다. STIX 형식을 사용하면 전역 위협 알림에서 위반 탐지 결과를 계층적 형식으로 표현할 수 있습니다. TAXII 서비스는 전역 위협 알림이 탐지한 인시던트를 STIX 언어 하위 집합을 사용하여 설명합니다. 현재 지원되는 개체는 다음과 같습니다.

- 캠페인-확인된 위협 범주(사용 가능한 경우)
- 인시던트-비정상적인 활동
- TTP-Tactics(전술), Techniques(기술), Procedures(절차)
- 관찰 가능 항목 - 웹 요청
- 지표 - 관찰 가능 조건을 식별하는 패턴

STIX에 관한 자세한 내용은 다음을 참조하십시오.

https://stix.mitre.org/

폴링 서비스

폴링 서비스는 표준화된 TAXII 전송 메커니즘을 사용하여 전역 위협 알림의 인시던트 정보를 TAXII 표준을 지원하는 클라이언트로 전송합니다. TAXII 클라이언트는 인시던트 정보를 가져오기 위해 TAXII 폴링 서비스에 폴링 요청을 전송합니다. HTTP 기본 인증은 권한 있는 사용자만 액세스할 수 있게 하는 데 사용합니다. 그러면 TAXII 폴링 서비스는 전역 위협 알림의 인시던트 정보를 TAXII 클라이언트로 전송하여 응답합니다. HTTPS 프로토콜은 모든 데이터 전송을 보호하는 데 사용합니다.

SIEM 또는 기타 보안 워크플로 시스템은 STIX/TAXII를 기본적으로 지원해야 합니다. TAXII 폴링 서비스를 주기적으로 폴링하도록 서드파티 TAXII 클라이언트를 구성하십시오.

- 계정 정보를 가져오려면 STIX/TAXII 서비스를 요청하십시오.
  1. 페이지 오른쪽 상단에 있는 전역 설정 톱니바퀴 아이콘을 클릭합니다.
  2. **CTA STIX/TAXII API**를 클릭합니다.
  3. **Add account(**계정 추가**)** 버튼을 클릭합니다.
  4. 계정을 식별하기 위한 이름을 입력하고 **Add account(**계정 추가**)** 버튼을 클릭합니다.
- 프로비저닝 프로세스가 완료되면 계정 정보가 표시됩니다. 창을 닫기 전에 이 계정 정보를 안전한 곳에 복사하십시오.

참고 보안 유지를 위해 비밀번호는 한 번만 표시됩니다. 비밀번호를 분실했다면 기존 비밀번호를 취소하고 새 비밀번호를 만들어야 합니다.

- 고유한 속성을 서드파티 TAXII 클라이언트에 복사합니다.

- pollEndpoint 또는 피드 서비스
  URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
- 사용자 이름
- 비밀번호
- 컬렉션 이름 또는 피드 이름

참고 2018년 8월 Cognitive Intelligence(구 Cognitive Threat Analytics 또는 CTA)가 Amazon Web Services의 새 위치로 마이그레이션하기 시작했으며, 그 결과 서비스에 액세스하고 서비스를 사용하는 데 필요한 새 IP 주소 및 추가 URL이 생성되었습니다. 서비스에 대한 액세스를 유지하려면 아웃바운드 방화벽 규칙을 업데이트해야 할 수 있습니다. 2018년 11월의 전환이 끝나면 이전 데이터 수집 서비스 IP 주소로 데이터를 전송할 수 없습니다. 필요한 변경 사항 및 기타 중요 정보에 관한 구체적인 세부 정보는 Field Notice(현장 알림)에서 확인할 수 있습니다.

참고 Cisco에서는 서드파티 제품 또는 SIEM 디바이스 구성 관련 기술 지원을 제공하지 않습니다. 문제가 있다면 벤더별 지원팀에 문의하십시오.

Cisco에서 TAXII 클라이언트 예시를 다운로드하여 사용하는 방법도 있습니다. SIEM 또는 기타 보안 시스템이 STIX/TAXII를 기본적으로 지원하지 않는 경우, Cisco는 SIEM 옆에 있는 Linux 또는 Windows VM 환경에 구축할 수 있는 경량 Java TAXII Log Adapter를 제공합니다. 제공된 링크를 클릭하여 설정 지침을 확인합니다. 이 어댑터는 TAXII API를 사용하여 새로운 인텔리전스의 정기 폴링을 수행하고 STIX 메시지에 데이터를 전달합니다. 그런 다음 어댑터가 STIX 메시지를 일반 SIEM 시스템에서 허용되는 다른 형식으로 변환합니다.

폴링 서비스의 안정성, 성능 및 가용성을 지원하려면 다음 조건이 충족되어야 합니다.

- 단일 TAXII 클라이언트의 폴링 요청은 10분마다 한 번만 허용됩니다. 그렇지 않으면 이 오류를 나타내는 상태 메시지가 반환됩니다.
- 각 폴링 요청은 최대 3일 동안의 인시던트 정보를 검색할 수 있습니다.
- 인시던트 정보는 검색을 위해 최대 30일 동안 저장됩니다.

폴링 요청

다음은 TAXII 클라이언트가 TAXII 폴링 서비스에 보내는 폴링 요청의 예입니다.

메서드는 POST입니다.

HTTP 요청 헤더:

```
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 ...
```

요청 본문:

```
<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>
```

지원되는 요청 매개변수	설명
Poll_Request	
message_id	TAXII 사양에 따라 각 요청에 대해 임의로 생성된 문자열입니다. 모든 요청에 대해 고유한 문자열을 재생성합니다.
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
exclude_Begin_Timestamp	기간에 따라 이 값을 조정합니다.
Inclusive_End_Timestamp	기간에 따라 이 값을 조정합니다.
Poll_Parameters	
allow_async	이 특성은 항상 false로 설정합니다.

참고 **Exclusive_Begin_Timestamp**와 **Inclusive_End_Timestamp** 사이에 허용되는 최대 기간은 3일입니다. 기간이 더 길면 반환되는 결과는 **Inclusive_End_Timestamp** 이전 3일로 제한됩니다.

폴링 응답

다음은 TAXII 폴링 서비스가 TAXII 클라이언트에 보내는 폴링 응답의 예입니다.

HTTP 응답 헤더:

```
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
```

응답 본문:

```
<?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>
```

참고 `Poll_Reponse`에 추가 위협 항목이 없다면, `more`과 `result_id`라는 두 속성이 존재하지 않습니다. `more=true`가 존재한다면, `Poll_Fulfillment`를 사용하여 응답의 다음 페이지를 요청할 수 있습니다.

지원되는 응답 개체	필드 설명
Poll_Response	
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
result_id	이 값을 폴링 이행 요청에 복사합니다.
exclude_Begin_Timestamp	이 폴링 응답이 적용되는 시간 범위의 시작 지점(지점 제외)입니다. 이 필드가 없다면 설문조가 응답이 이 TAXII 데이터 피드에 대한 가장 빠른 시간을 포함한다는 뜻입니다.
Inclusive_End_Timestamp	이 폴링 응답이 적용되는 시간 범위의 종료 지점(지점 포함)입니다.
Content_Block	반환된 콘텐츠입니다.
Content_Binding	
콘텐츠	
STIX_Package	STIX 언어 관련 정보입니다.

지원되는 응답 개체	필드 설명
STIX_Header	이 STIX 콘텐츠 패키지에 관한 정보입니다.
인시던트	하나 이상의 인시던트입니다.
사고	단일 인시던트 관련 정보입니다.
직함	이 인시던트를 설명하는 제목입니다.
피해자	이 인시던트의 피해자에 관한 정보입니다.
Related_Indicators	이 인시던트와 관련된 지표를 식별합니다.
Related_Indicator	이 인시던트와 관련된 단일 지표를 식별합니다.
지표	특정 관찰 가능 조건과 패턴의 의미에 대한 상황별 정보, 조치 방법 및 시점 등에 관한 정보를 식별하는 패턴으로 구성된 지표입니다.
관찰 가능 항목	이 지표와 관련된 관찰 가능 항목입니다.
Observable_Composition	다른 관찰 가능 항목의 논리적 조합을 작성하여 고차 복합 관찰 가능 항목을 지정할 수 있게 합니다.
관찰 가능 항목	단일 관찰 가능 항목을 나타냅니다.
객체	특정 개체의 특성(예: 파일, 레지스트리 키, 프로세스)을 식별합니다.
속성	개체에 대한 작업의 결과로 열거된 속성입니다.
Custom_Properties	기존 Properties(속성) 스키마에 정의되어 있지 않은 사용자 지정 개체 속성 집합을 지정할 수 있게 합니다.
속성	개체에 대한 작업의 결과로 열거된 단일 속성입니다.
Indicatord_TTP	이 지표가 나타내는 관련 TTP(Tactics, Techniques, and Procedures)를 지정합니다.
Discovery_Method	코드를 검색하는 데 사용하는 방법 및/또는 툴에 관한 정보입니다.
COA_Requested	이 인시던트에 권장되는 조치입니다.
신뢰	이 인시던트의 특성에 대한 신뢰도 수준 관련 정보입니다.

지원되는 응답 개체	필드 설명
Information_Source	이 인시던트의 소스 관련 정보입니다.
툴	
Tool(툴)	이 인시던트를 탐지한 툴(CTA 또는 AMP)입니다.

오류가 발생하면 오류 메시지가 반환됩니다. 예를 들면 다음과 같습니다.

```
<?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	오류 설명
	사용자가 인증되지 않음, HTTP 응답 상태 코드 404
DENIED	사용자에게 권한이 부여되지 않음, HTTP 응답 상태 코드 401
BAD_MESSAGE	잘못된 요청 메시지입니다. `Message` 매개변수를 참조하십시오.
FAILURE	지정되지 않은 오류입니다. `Message` 매개변수를 참조하십시오.

폴링 이행

다음은 TAXII 클라이언트가 TAXII 폴링 서비스에 보내는 폴링 수행 요청의 예입니다.

메서드는 POST입니다.

HTTP 요청 헤더:

```
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 ...
```

요청 본문:

```
<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>
```

지원되는 요청 매개변수	설명
Poll_Request	
message_id	TAXII 사양에 따라 각 요청에 대해 임의로 생성된 문자열입니다. 모든 요청에 대해 고유한 문자열을 재생성합니다.
collection_name	전역 위협 알림 서비스에서 추출하거나 가져올 컬렉션의 이름입니다. 이 속성은 프로비저닝 프로세스가 완료된 후 Cisco에서 제공합니다.
result_id	폴링 응답에서 이 값을 붙여넣습니다.
result_part_number	폴링 응답의 값에서 1 높은 값을 이 값으로 만듭니다.
exclude_Begin_Timestamp	기간에 따라 이 값을 조정합니다.
Inclusive_End_Timestamp	기간에 따라 이 값을 조정합니다.
Poll_Parameters	
allow_async	이 특성은 항상 false로 설정합니다.

참고 **Exclusive_Begin_Timestamp**와 **Inclusive_End_Timestamp** 사이에 허용되는 최대 기간은 3일입니다. 기간이 더 길면 반환되는 결과는 **Inclusive_End_Timestamp** 이전 3일로 제한됩니다.

일반 쿼리

이 섹션에서는 추가 조사를 위해 결과의 우선 순위를 지정하는 데 도움이 되는, Cisco STIX/TAXII API에서 사용하는 몇 가지 일반적인 쿼리에 대해 설명합니다. 예제 쿼리에서 사용하는 구문은 SPLUNK

통합을 기반으로 하며, 상징적입니다. 구체적인 필드와 값은 로컬 통합에 따라 달라질 수 있지만, 쿼리의 의미는 SIEM 시스템 및 통합 전반에 광범위하게 적용됩니다.

팁 SPLUNK에서 다른 데이터를 수집한다면, 전역 위협 알림 데이터를 통해서만 검색될 수 있도록 호스트, 인덱스 또는 소스 이름을 쿼리 앞에 추가하십시오.

확인된 위협의 영향을 받는 사용자

이 쿼리는 확인된 위협이 있는 모든 사용자를 반환하며, 데스크톱 치료를 위해 인시던트 대응 팀에 보고될 수 있습니다. 인시던트의 위험성이 높다면 영향 받는 디바이스의 이미지 재설치를 고려해야 합니다. 이 쿼리는 영향을 받는 사용자 이름 및 캠페인 이름이 포함된 표를 생성합니다. 비어 있지 않은 캠페인 이름을 검색한 다음 사용자 이름+캠페인 쌍을 중복 제거합니다.

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

또는 캠페인 이름에 다중 값 필드를 사용합니다.

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

특정 기간 내에 확인된 위협의 영향을 받는 사용자

이 쿼리에는 first-seen 및 last-seen 열도 포함됩니다. 비어 있지 않은 캠페인을 검색하고, 사용자 이름+캠페인 쌍으로 집계하고, 웹 플로우 타임스탬프의 최소값과 최대값을 계산합니다. 결과는 에포크-밀리초 단위로 표시되며 필요하다면 달력 시간으로 변환할 수 있습니다.

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

strftime 함수를 사용하여 에포크 변환을 포함할 수도 있습니다. 이 예에서는 타임스탬프를 1000으로 나눠 밀리초를 제거합니다.

```
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
```

높은 위험 및 높은 신뢰도 인시던트의 영향을 받는 사용자

이 쿼리는 확인된 캠페인 보유 여부에 관계없이 높은 위험 및 높은 신뢰도 사용자의 우선순위 목록 테이블을 생성합니다. 높은 위험, 높은 신뢰도 및 중복 사용자 이름을 검색합니다. 모든 인시던트의 위험과 신뢰도 수준이 모두 높으니, 영향 받는 디바이스의 이미지 재설치를 고려해야 합니다.

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

캠페인의 영향을 받는 사용자

이 쿼리는 시간 경과에 따른 감염된 사용자 수를 캠페인별로 분류한 차트를 생성합니다. 비어 있지 않은 캠페인을 검색하여 1일 기간으로 비운 다음, 해당 빈에 있는 고유한 사용자 이름 수를 계산합니다.

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

참고 SPLUNK에서는 시간 차트 바로 가기를 사용할 수 있습니다.

C&C(Command and Control) 서버

이 쿼리는 Confirmed(확인됨) 범주에 속하는 모든 탐지된 C&C(명령 및 제어) 서버의 목록을 생성합니다. 서버 IP 주소 및 캠페인을 표시하는 비어 있지 않은 캠페인을 검색한 다음 서버 IP 주소를 중복 제거합니다. 결과에는 C&C 통신을 유지하기 위해 감염된 디바이스에서 사용 중인 C&C IP 수신 주소가 나열됩니다. 각 C&C IP 주소와 관련된 위협 캠페인도 표시됩니다. 다른 시스템을 쿼리하여 추가 정보를 얻고, IOC(보안 침해 지표)를 제공하고, 감염된 엔드포인트에서 악성 프로세스 및 애플리케이션을 식별하는 데 사용할 수 있습니다.

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

Cisco ISE와의 통합

Cisco ISE(71Introduction)는 네트워크 리소스에 대한 보안 액세스를 제공하는 보안 정책 관리 플랫폼입니다. Cisco ISE는 정책 결정 지점 역할을 하고, 기업이 규정을 준수하고, 인프라 보안을 개선하고, 서비스 작업을 효율화할 수 있도록 합니다. Cisco ISE를 사용하는 기업은 네트워크, 사용자 및 디바이스에서 실시간 상황별 정보를 수집할 수 있습니다. 그런 다음 이 정보를 사용하여 네트워크의 다양한 요소에 ID를 연결하여 사전 대응적 거버넌스 결정을 내릴 수 있습니다.

전역 위협 알림은 Cisco ISE와 통합되어 네트워크 수준의 격리를 제공합니다. 이 격리는 민감한 데이터가 더 이상 추출되지 감염된 디바이스를 않도록 네트워크에서 차단하는 기능을 제공합니다. 글로벌 위협 알림과 Cisco ISE의 통합은 STIX/TAXII를 사용합니다. 시스템이 감염의 원인을 개별 사용자에게 돌릴 수 있는 중요도가 높은 위험을 발견한 경우, Cisco ISE는 Cisco Rapid Threat Containment 프레임워크의 일부인 TC-NAC(Threat Centric Network Access Control) Quarantine을 제안하는 Requested Course of Action(요청된 조치)을 수신합니다. 감염과 관련된 위험에 따라, Requested Course of Action(요청된 조치)은 모니터링, 박멸, 내부 차단 또는 이러한 요소의 조합일 수 있습니다. 내부 차단은 TC-NAC의 차단 정책에서 사용하는 행동 방침입니다. 자세한 내용은 Cisco Rapid Threat Containment를 참고하십시오.

Cisco ISE와 전역 위협 알림 STIX/TAXII 서비스에서 제공하는 데이터 피드를 사용하여 고유한 솔루션을 개발할 수 있습니다. 데이터 피드에는 감염된 디바이스 및 수행할 작업을 식별하는 방법에 대한 정보가 포함되어 있습니다. 전역 위협 알림 STIX/TAXII 피드의 권장 사항을 기준으로 Cisco ISE에서 격리 정책을 정의할 수 있습니다. Cisco ISE에서 전역 위협 알림 어댑터를 구성하는 방법에 대한 자세한 내용은 Cisco ISE 관리자 가이드, 릴리스 2.2를 참조하십시오.

참고 전역 위협 알림은 웹 프록시 로그에 클라이언트 IP 또는 사용자 이름으로 나열되는 사용자 ID를 이용해 작동합니다. 특히 IP 주소의 경우 프록시 로그를 통해 사용 가능한 IP 주소가 내부 기업 네트워크에서 (다른 디바이스를 위한) 다른 IP 주소와 충돌하는 IP 주소일 수 있습니다. 예를 들어 인터넷에 바로 연결되는 스플릿 터널이 있는 AnyConnect를 통해 연결된 로밍 사용자는 집에서 로컬 IP 주소(예: 10.0.0.x 주소)를 얻게 되는데, 이 주소가 내부 기업 네트워크에서 사용하는 중복된 프라이빗 범위에 있는 IP 주소와 충동할 수 있습니다. Rapid Threat Containment(신속한 위협 억제) 정책을 정의할 때는 일치하지 않는 디바이스에 격리 작업이 적용되지 않게 하는 논리적 네트워크 아키텍처를 고려해야 합니다.