STIX/TAXII 服务

概述

全局威胁警报允许您将检测到的事件的相关信息提取到客户端，以进行进一步的关联分析和存档。该服务支持 MITRE 的指标信息的可信自动化交换 (TAXII) 标准，用于与安全信息和事件管理 (SIEM) 系统集成。TAXII 标准指定用于在系统之间共享网络威胁信息的传输机制。

有关 TAXII 的详细信息，请参阅：

TAXII MITRE 组织

TAXII 项目 GitHub

使用结构化威胁信息表示式 (STIX) 语言格式表示每个事件中的信息。STIX 是一种结构化语言，用于描述网络威胁信息，以便以一致的方式共享、存储和分析这些信息。STIX 格式允许全局威胁警报以分层格式表示其漏洞检测结果。TAXII 服务使用 STIX 语言的子集描述全局威胁警报检测到的事件。目前，支持的对象包括：

- 活动—已确认威胁类别（如果可用）
- 事件—异常活动
- TTP—策略、技术和流程
- 可观察条件—Web 请求
- 指示器—识别可观察条件的模式

有关 STIX 的详细信息，请参阅：

https://stix.mitre.org/

轮询服务

轮询服务使用标准化 TAXII 传输机制，以将事件信息从全局威胁警报发送到支持 TAXII 标准的客户端。要提取事件信息，TAXII 客户端需向 TAXII 轮询服务发送轮询请求。HTTP 基本身份验证仅用于限制授权用户的访问权限。然后，TAXII 轮询服务通过将来自全局威胁警报的事件信息发送到 TAXII 客户端进行响应。HTTPS 协议用于保护所有数据传输的安全性。

您的 SIEM 或其他安全工作流程系统必须能够本地支持 STIX/TAXII。将第三方 TAXII 客户端配置为定期轮询 TAXII 轮询服务。

- 要获取您的帐户信息，请求 STIX/TAXII 服务。
  - 点击右上角的全局设置齿轮图标。
  - 点击 **CTA STIX/TAXII API**。
  - 点击**添加帐户**按钮。
  - 输入名称以标识您的帐户，然后点击**添加帐户**按钮。
- 完成配置过程后，系统将显示您的帐户信息。在关闭窗口之前，请将此帐户信息复制到安全位置。

注释 出于安全原因，加密密码仅显示一次。如果丢失加密密码，则必须撤销现有加密密码并生成新的加密密码。

- 将唯一属性复制到第三方 TAXII 客户端中：
  - pollEndpoint 或源服务 URL=`https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService`
  - 用户名
  - 密码
  - 集合名称或源名称

注释 2018 年 8 月，感知智能（以前称为感知威胁分析或 CTA）开始迁移到 Amazon Web Services 中的新位置，从而产生新的IP地址和访问和使用该服务的额外URL。要保持对服务的访问，可能需要更新出站防火墙规则。在 2018 年 11 月切换后，您将无法再将数据成功发送到旧的数据注入服务 IP 地址。有关所需更改和其他重要信息的具体详细信息，请参阅现场通知。

注释 我们不为配置第三方产品或SIEM设备提供技术支持。如果出现问题，请咨询特定供应商支持团队。

或者，您可以从思科下载并使用示例 TAXII 客户端。如果您的 SIEM 或其他安全系统本地不支持 STIX/TAXII，思科会提供一个轻量级 Java TAXII 日志适配器，您可以将其部署到 SIEM 旁边的 Linux 或 Windows VM 环境。点击提供的链接以查看设置说明。适配器使用 TAXII API 对任何新情报执行定期轮询，并在 STIX 消息中传送数据。然后，适配器将 STIX 消息转换为常见 SIEM 系统接受的其他格式。

要实现轮询服务的稳定性、性能和可用性，请执行以下操作：

- 每 10 分钟内仅允许来自任何单个 TAXII 客户端的一个轮询请求。否则，将返回指示此错误的状态消息。
- 每个轮询请求可以检索长达三天的事件信息。
- 存储的事件信息最多可检索 30 天。

轮询请求

以下是从您的 TAXII 客户端到 TAXII 轮询服务的轮询请求示例。

方式为 POST。

HTTP 请求信头：

```
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 ...
```

请求正文：

```
<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>
```

支持的请求参数	说明
Poll_Request	
message_id	根据 TAXII 规范为每个请求随机生成的字符串。重新生成每个请求的唯一字符串。

支持的请求参数	说明
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
Exclusive_Begin_Timestamp	根据您的时间范围调整此值。
Inclusive_End_Timestamp	根据您的时间范围调整此值。
Poll_Parameters	
allow_asynch	始终将此属性设置为 false。

注释 **Exclusive_Begin_Timestamp** 和 **Inclusive_End_Timestamp** 之间支持的最大差值为三天。如果差值较大，则返回的结果限于 **Inclusive_End_Timestamp** 之前的最后三天。

轮询响应

以下是从 TAXII 轮询服务到 TAXII 客户端的轮询响应示例。

HTTP 响应信头：

```
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
```

响应正文：

```
<?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>
```

注释 在 `Poll_Reponse` 中，如果没有更多威胁项目，则 `more` 和 `result_id` 这两个属性不存在。当 `more=true` 存在时，您可以使用 `Poll_Fulfillment` 请求响应的下一页。

支持的响应对象	字段说明
Poll_Response	
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
result_id	将此值复制到轮询执行请求。
Exclusive_Begin_Timestamp	此轮询响应涵盖的时间范围的排他性起点。缺少此字段表示轮询响应涵盖此 TAXII 数据源的最早时间。
Inclusive_End_Timestamp	此轮询响应覆盖的时间范围的包含端。
Content_Block	返回的内容。
Content_Binding	
内容	
STIX_Package	有关 STIX 语言的信息。
STIX_Header	有关 STIX 内容包的信息。
突发事件	一个或多个事件。
事故	有关单个事件的信息。
标题	描述此事件的标题。
受害者	有关此事件的受害者的信息。
Related_Indicators	标识与此事件相关的指示器。
Related_Indicator	标识与此事件相关的单个指示器。
指标	指示器由识别特定可观察条件的模式以及有关模式含义、应如何实施和何时执行操作等的情景信息组成。
可观察	此指示器的相关可观察对象。
Observable_Composition	允许通过组合其他可观察对象的逻辑组合，来指定更高层次的复合可观察对象。
可观察	表示单个可观察对象。
对象	识别特定对象（例如文件、注册表密钥、流程）的特征
属性	对对象执行操作时枚举的属性。

支持的响应对象	字段说明
Custom_Properties	启用指定一组可能在现有属性架构中未定义的自定义对象属性。
属性	对对象执行操作时枚举的单个属性。
Indicated_TTP	指定此指示器指示的相关战术、技术和程序 (TTP)。
Discovery_Method	有关用于发现代码的方法和/或工具的信息。
COA_Requested	针对此事件的建议操作步骤。
置信	有关表征此事件的置信度的信息。
Information_Source	有关此事件来源的信息。
工具	
工具	哪个工具（CTA 或 AMP）检测到此事件。

如果出现错误，则将返回错误消息。例如：

```
<?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	错误说明
	用户未通过身份验证，HTTP 响应状态代码为 404
DENIED	用户未通过授权，HTTP 响应状态代码为 401
BAD_MESSAGE	请求消息无效，请参阅消息参数
失败	未指定错误，请参阅消息参数

轮询执行

以下是从您的 TAXII 客户端到 TAXII 轮询服务的轮询执行请求示例。

方式为 POST。

HTTP 请求信头：

```
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 ...
```

请求正文：

```
<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>
```

支持的请求参数	说明
Poll_Request	
message_id	根据 TAXII 规范为每个请求随机生成的字符串。重新生成每个请求的唯一字符串。
collection_name	要从全局威胁警报服务提取的集合的名称。此属性将在调配过程完成后由思科提供给您。
result_id	从轮询响应中粘贴此值。
result_part_number	将此值从轮询响应中的值增加 1。
Exclusive_Begin_Timestamp	根据您的时间范围调整此值。
Inclusive_End_Timestamp	根据您的时间范围调整此值。
Poll_Parameters	
allow_asynch	始终将此属性设置为 false。

注释 **Exclusive_Begin_Timestamp** 和 **Inclusive_End_Timestamp** 之间支持的最大差值为三天。如果差值较大，则返回的结果限于 **Inclusive_End_Timestamp** 之前的最后三天。

常规查询

本节介绍思科 STIX/TAXII API 中使用的一些常见查询，以帮助确定调查结果的优先顺序，以便进一步调查。示例查询中使用的语法基于 SPLUNK 集成并，为符号。特定字段和值可能因本地集成而异，但查询的含义广泛适用于 SIEM 系统和集成。

提示 如果您正在收集 SPLUNK 中的其他数据，请在主机名、索引或源名称前添加查询，以仅搜索全局威胁警报数据。

受到已确认威胁影响的用户

此查询将返回带有已确认威胁的所有用户，并且可能会报告给事件响应团队进行桌面补救。如果这些事件也具有高风险，请考虑重新映像受影响的设备。此查询将生成一个表格，其中包含受其影响的用户名和活动名称。搜索非空活动名称，然后删除重复的用户名+活动对：

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

或者，使用活动名称的多值字段：

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

在一个时间段内受到已确认威胁影响的用户

此查询还包括“首次发现”和“最后发现”列。搜索非空活动，按用户名+活动对进行汇总，并计算网络流时间戳的最小值和最大值。结果以纪元毫秒为单位，如果需要，可以转换为日历时间。

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

或者，使用 strftime 函数包含纪元转换。此示例将时间戳除以 1000 以删除毫秒：

```
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
```

受高风险和高置信度事件影响的用户

此查询生成高风险和高置信度用户的优先级列表，无论他们是否有已确认的活动。搜索高风险、高置信度和重复数据删除的用户名。由于所有这些事件都具有高风险和高置信度，因此请考虑重新映像受影响的设备。

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

受活动影响的用户

此查询将生成一个图表，显示一段时间内受感染用户的数量，并按活动细分。搜索非空活动，按一天的时间间隔归纳数据，并计算该收集器中的不同用户名计数。

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

注释 在 SPLUNK 中，可以使用时间表快捷方式。

命令和控制服务器

此查询生成“已确认”类别中所有检测到的命令和控制 (C&C) 服务器的列表。搜索非空活动，同时显示服务器 IP 地址和活动，然后对服务器 IP 地址进行重复数据删除。此结果列出了受感染设备的 C&C IP 目标地址以用于维护 C&C 通信。对于每个 C&C IP 地址，您还可以查看其涉及的威胁活动。可用于查询其他系统以获取更多情报，提供感染指标 (IOC) 以及识别受感染终端上的恶意进程和应用。

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

与思科 ISE 的集成

思科身份服务引擎 (ISE) 是一种可用于安全地访问网络资源的安全策略管理平台。思科 ISE 是一个策略决策点，可帮助企业确保合规，加强基础设施安全以及简化服务操作。通过思科 ISE，企业可以从网络、用户和设备收集实时情境信息。然后，您可以通过将身份绑定到网络中的各种元素，使用该信息做出前瞻性的管理决策。

全局威胁警报与思科ISE集成以提供网络级隔离，该功能具有从网络中删除受感染设备的功能，这样就无法进一步泄露敏感数据。全局威胁警报与思科 ISE 之间的集成使用 STIX/TAXII。对于系统能够将感染归因于单个用户的关键级别风险发现，思科 ISE 会收到请求的操作过程，该过程建议威胁中心网络访问控制 (TC-NAC) 隔离，这隶属于思科快速威胁遏制框架。根据与感染相关的风险，请求的操作过程可以是监控、根除、内部阻止或组合。内部阻止是要在 TC-NAC 中的阻止策略中使用的操作过程。有关详细信息，请参阅思科快速威胁遏制。

您可以使用思科 ISE 和全局威胁警报 STIX/TAXII 服务提供的数据源来开发自己的解决方案。数据源包含有关识别受感染设备和要执行的操作的信息。您可以根据全局威胁警报STIX / TAXII源中的建议在思科ISE中定义隔离策略。有关如何在思科ISE中配置全局威胁警报适配器的信息，请参阅《思科ISE管理员指南，版本2.2》。http://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22.html

注释 全局威胁警报使用 Web 代理日志中作为客户端 IP 或用户名列出的用户身份。具体而言，在使用 IP 地址的情况下，通过代理日志可用的 IP 地址可能是与内部企业网络上另一个 IP 地址（用于另一台设备）冲突的 IP 地址。例如，通过 AnyConnect 和分割隧道直接连接到互联网的漫游用户可以在家中获取本地 IP 地址（例如，10.0.0.x 地址），该地址可能与内部企业网络中使用的重叠私用范围中的 IP 地址冲突。当您定义快速遏制威胁策略时，请考虑您的逻辑网络架构，以避免将隔离操作应用于不匹配的设备。