TAXII Service

Overview

Cisco ScanCenter allows you to pull information on incidents detected by CTA down to your client for further analysis and archival. The service supports MITRE's Trusted Automated eXchange of Indicator Information (TAXII) standard. The TAXII standard specifies transport mechanisms used to share cyber threat information between systems.

For information on TAXII, see:

https://taxii.mitre.org/

The information in each incident is represented using the Structured Threat Information eXpression (STIX) language format. The TAXII service uses a subset of the STIX language to describe the incidents CTA has detected. Currently, the supported objects include:

- Campaign—Confirmed threat category, if available
- Incident—Anomalous activity
- TTP—Tactics, Techniques, and Procedures
- Observable—Web requests
- Indicator—Pattern identifying observable conditions

For information on STIX, see:

https://stix.mitre.org/

Poll Service

The TAXII poll service uses standardized transport mechanisms to share incident information between CTA and clients supporting the TAXII standard. To pull incident information, the TAXII client sends a poll request to the TAXII poll service. HTTP basic authentication is used to restrict access for authorized users only. The username and password are sent in every HTTP request. The TAXII poll service then responds by sending incident information to the TAXII client. HTTPS protocol is used to secure all data transfers.

An example TAXII client is the SPLICE plugin which integrates into the SIEM platform SPLUNK. The SPLICE plugin allows you to feed STIX information into SPLUNK for analysis. For information on how to use SPLICE in SPLUNK, see:

https://apps.splunk.com/app/1870/

Note We do not provide technical support for configuring third-party products or SIEM devices. In the event of an issue, consult the vendor-specific support team.

Configure your third-party TAXII client to periodically poll the TAXII poll service.

- To obtain your credentials, request TAXII service in ScanCenter. <Add UI details>
- After the provisioning process is completed, your credentials will be sent to you in ScanCenter. <Add UI details>
- Copy your unique attributes into your third-party TAXII client: collection_name, username, password <Add SPLUNK UI details>

Note To support the stability, performance, and availability of the poll service:

- Only one poll request from any single TAXII client is allowed within every 10 minutes. Otherwise, a status message indicating this error is returned.
- Each poll request may retrieve incident information spanning up to three days.
- Incident information is stored for retrieval for up to 30 days.

Poll Request

The following is an example of a poll request from your TAXII client to the TAXII poll service.

HTTP Request headers:

```
x-taxii-content-type: urn:taxii.mitre.org:protocol:http:1.0
x-taxii-protocol: urn:taxii.mitre.org:message:xml:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
authorization: Basic dXNlcjpwYXNz
content-type: application/xml; charset=UTF-8
```

Request body:

```
<taxii_1:Poll_Request xmlns:taxii_1="http://taxii.mitre.org/messages/taxii_xml_binding-1"
                           message_id="23537" collection_name="webflows_1234567890_v0">

<taxii_1:Exclusive_Begin_Timestamp>2015-01-16T00:00:00+00:00</taxii_1:Exclusive_Begin_Timestamp>

 <taxii_1:Inclusive_End_Timestamp>2015-01-17T00:00:00+00:00</taxii_1:Inclusive_End_Timestamp>

 <taxii_1:Poll_Parameters allow_asynch="false"/>
</taxii_1:Poll_Request>
```

Supported Request Parameters	Description
Poll_Request	

Supported Request Parameters	Description
collection_name	Name of collection to extract or pull from the CTA service. This attribute will be provided to you by Cisco after the provisioning process is completed.
Exclusive_Begin_Timestamp	
Inclusive_End_Timestamp	
Poll_Parameters	
allow_asynch	Always set this attribute to false.

Note The maximum supported difference between **Exclusive_Begin_Timestamp** and **Inclusive_End_Timestamp** is three days. In case the difference is more, the returned result is limited to the last three days before **Inclusive_End_Timestamp**.

Poll Response

The following is an example of a poll response from the TAXII poll service to the TAXII client.

HTTP Response headers:

```
x-taxii-content-type: urn:taxii.mitre.org:protocol:http:1.0
x-taxii-protocol: urn:taxii.mitre.org:message:xml:1.1
x-taxii-services: urn:taxii.mitre.org:services:1.1
```

Response body:

```
<?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: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="webflows_1234567890_v0" in_response_to="23537"
                 message_id="1d5b9aba-6233-4e55-abe1-80dc6b28fe13">
    <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: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>
```

Supported Response Objects	Description of Field
Poll_Response	
Exclusive_Begin_Timestamp	Exclusive beginning of the time range covered by this poll response. Absence of this field indicates that the poll response covers the earliest time for this TAXII data feed.
Inclusive_End_Timestamp	Inclusive end of the time range covered by this poll response.
Content_Block	Returned content.
Content_Binding	
Content	
STIX_Package	Information about the STIX language.
STIX_Header	Information about this package of STIX content.
Incidents	One or more incidents.
Incident	Information about a single incident.
Title	Title describing this incident.
Victim	Information about the victim of this incident.
Related_Indicators	Identifies indicators related to this incident.
Related_Indicator	Identifies a single indicator related to this incident.
Indicator	Indicator made up of a pattern that identifies certain observable conditions as well as contextual information about the pattern's meaning, how and when it should be acted upon, etc.

Supported Response Objects	Description of Field
Observable	Relevant observable for this indicator.
Observable_Composition	Enables specifying higher-order composite observables by composing logical combinations of other observables.
Observable	Represents a single observable.
Object	Identifying characteristics of a specific object (e.g. file, registry key, process)
Properties	Properties that were enumerated as a result of the action on the object.
Custom_Properties	Enables specifying a set of custom object properties that may not be defined in existing Properties schemas.
Property	A single property that was enumerated as a result of the action on the object.
Indicated_TTP	Specifies the relevant Tactics, Techniques, and Procedures (TTP) indicated by this indicator.
Discovery_Method	Information about the method and/or tool used to discover the code.
Confidence	Information about the level of confidence held in the characterization of this incident.
Information_Source	Information about the source of this incident.
Tools	
Tool	Which tool, CTA or AMP, detected this incident.

In case of an error, an error message is returned. For example:

```
<?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	Description of Error
	User is not authenticated, HTTP response status code of 404
DENIED	User is not authorized, HTTP response status code of 401
BAD_MESSAGE	Invalid request message, refer to `Message` parameter
FAILURE	Unspecified error, refer to `Message` parameter