Filtering Automated Indicator Sharing (AIS) Content Based on Specified Criteria

V1.0

Publication: December 2021
Cybersecurity and Infrastructure Security Agency

Contents

1 What are Filters?

Filters are a capability in the Trusted Automated Exchange of Intelligence Information (TAXII) specification that enable users to query and retrieve a subset of Structured Threat Information Expression (STIX) content from the entire set of STIX content on a TAXII server based on a set of parameters. While the TAXII specification currently defines a small subset of parameters by which STIX content can be filtered, AIS has expanded the set of match fields by which STIX content can be filtered beyond what is otherwise defined in the TAXII specification to better enable AIS participants to get the content that they need. Table 1 provides a list of parameters and fields that may be used as filters in the TAXII specification and AIS.

Table 1: Parameters and Match Filter Fields

Parameters	TAXII	AIS
added_after	X	X
limit	X	X
next	X	X
match[<field>]	X	X
match Fields		
confidence		X
created_by_ref		X
external_id		X
id	X	X
labels		X
object_marking_refs		X
object_refs		X
opinion		X
relationship_type		X
sectors		X
sighting_of_ref		X
source_name		X
source_ref		X
spec_version	X	X
target_ref		X
tlp		X
type	X	X
valid_on_after[1]		X
value		X
version	X	X

2 Why are Filters Important?

Hundreds of thousands of STIX objects are shared over AIS every year and are not equally relevant to all organizations. It takes time for an organization to triage them and determine if action should be taken. Filters assist analysts in the triage process and allow them to extract a smaller subset of the overall AIS feed to

[1] Customized AIS field that considers the valid_from, valid_until, and revoked properties of Indicator objects.

prioritize the STIX objects that are most likely to be actionable in support of their organization's network defense.

3 Using Filters

The examples below show how filters can be used to limit what STIX content gets retrieved from the AIS TAXII server.[2] All the filters in these examples fall under the "match" parameter, where the filter field name is included in brackets after the keyword "match." For example, the following filter matches content that corresponds (by object type) to an Indicator object:

?match[type]=indicator

All filters can match against multiple values by separating the values by a comma; if multiple values are given, the comma is treated as a logical OR operator, meaning objects with any of the listed values will be returned. For example, the following filter matches content that corresponds to either an Indicator OR a Course of Action (COA) object; the results returned would include all Indicator and COA objects:

?match[type]=indicator,course-of-action

All filters can be further narrowed, by any number of characteristics, by using an "&" without any spaces. If multiple parameters are present, the & is treated as a logical AND operator. For example, the following filter matches content that is both an Indicator object AND has a confidence value of 90:

?match[type]=indicator&match[confidence]=90

It is worth noting that many of these filters are for specific properties of STIX objects, which means that you may be filtering for a property that is not defined for, or may not be included in, all objects; in such cases, objects without the property will not be returned by the request. Also, these examples are illustrative only, and the values may be modified to obtain different results that satisfy each analyst's requirements.

4 Use Cases

For illustrative purposes, this document divides example use cases into four categories, though there may be other use cases for leveraging filtering or the examples provided.

4.1 Hunt

Use cases that a threat hunter might use to identify or understand specific indicators of compromise or vulnerabilities, or related tactics, techniques, and procedures or defensive measures.

4.2 Research

Use cases that an analyst might use to obtain a broader understanding (i.e. context) of the cyber threat intelligence shared by the AIS community.

4.3 Trust

Use cases that an analyst might use to evaluate the relevance of AIS data. For example, trust use cases relate to content created by specific organizations that are trusted by the analyst, as well as confidence scores and opinion values.

[2] https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html#_Toc31107517

4.4 Advanced

Use cases that an analyst might use that require multi-step filters.

The following is a mapping between the match fields available for filtering in AIS and the respective use case category where application of the match field is illustrated in this document.

Table 2: Mapping of Match Filter Fields to Categories Where Use Case is Illustrated

match Fields	Category
confidence	Trust
created_by_ref	Trust
external_id	Research
id	Hunt
labels	Research
object_marking_refs	Research
object_refs	Hunt
opinion	Trust
relationship_type	Hunt
sectors	Research
sighting_of_ref	Hunt
source_name	Research
source_ref	Hunt
spec_version	Research
target_ref	Hunt
tlp	Research
type	Hunt
valid_on_after[3]	Trust
value	Hunt

When objects meeting filtered criteria reference other objects, multiple queries will need to be made to obtain both the set of objects directly meeting the filtering criteria and the referenced objects, because TAXII filtering only returns the objects that match the filter directly; filtering does not drill down and return all matching objects and all referenced objects within matching objects. Examples of such complex use cases are contained in the Advanced Use Cases section.

5 Hunt Use Cases

The following examples support use cases that a threat hunter might use to identify or understand specific indicators of compromise or vulnerabilities, or related tactics, techniques, and procedures or defensive measures.

[3] Considers the valid_from, valid_until, and revoked properties of Indicator objects.

5.1 Relationship Pivoting

These filters retrieve Relationship objects with a specific source or target object and/or a specific relationship type. A Relationship object defines directional links between two STIX objects and specifies how the two objects are related[4,5] via the **source_ref**, **target_ref**, and **relationship_type** properties. The following filters identify Relationship objects based on these properties.

5.1.1 Relationship source reference

?match[type]=relationship&match[source_ref]=<identifier>

For example, the filter,

?match[type]=relationship&match[source_ref]= indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7

will return the Relationship object shown in Figure 1, as well as all other Relationship objects that reference the specified Indicator object as the source.[6]


```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--df7c87eb-75d2-4948-af81-9d49d246f301",
  "created": "2016-04-06T20:06:37.000Z",
  "modified": "2016-04-06T20:06:37.000Z",
  "relationship_type": "indicates",
  "source_ref": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "target_ref": "malware--9c4638ec-f1de-4ddb-abf4-1b760417654e"
}
```


Figure 1: Relationship object ("indicates")

Output: Relationship objects with the Indicator object (indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7) as the source.

5.1.2 Relationship target reference

?match[type]=relationship&match[target_ref]=<identifier>

For example, the filter,

?match[type]=relationship&match[target_ref]=malware--9c4638ec-f1de-4ddb-abf4-1b760417654e

will return the Relationship object in Figure 1, as well as all other Relationship objects that reference the specified Malware object as the target.[7]

Output: Relationship objects with the Malware object (malware--9c4638ec-f1de-4ddb-abf4-1b760417654e) as the target.

[4] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_e2e1szrqfoan
[5] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_6n2czpjuie3v
[6] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_muftrcpnf89v
[7] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_s5l7katgbp09

5.1.3 Relationship type and target reference

?match[relationship_type]=<string>&match[target_ref]=<identifier>

For example, the filter,

?match[relationship_type]=mitigates&match[target_ref]=vulnerability--9c4638ec-f1de-4ddb-abf4-1b760417654e

will return the Relationship object shown in Figure 2, as well as all other Relationship objects that are identified in the **relationship_type** property as mitigating (**mitigates**) the specified target vulnerability.[8]


```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--df7c87eb-75d2-4948-af81-9d49d246f301",
  "created": "2016-04-06T20:06:37.000Z",
  "modified": "2016-04-06T20:06:37.000Z",
  "relationship_type": "mitigates",
  "source_ref": "course-of-action--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "target_ref": "vulnerability--9c4638ec-f1de-4ddb-abf4-1b760417654e"
}
```


Figure 2: Relationship object ("mitigates")

Output: Relationship objects of relationship type "mitigates" with the Vulnerability object (vulnerability--9c4638ec-f1de-4ddb-abf4-1b760417654e) as the target.

5.2 Sighted Indicators

This filter retrieves Sightings of a specific object. Sighting objects represent cyber threat intelligence believed to have been seen.[9] Sightings can be used by organizations to determine what is being seen in the wild and who is being targeted. The following filter demonstrates how relevant sightings can be returned by leveraging the **sighting_of_ref** property.

5.2.1 Sighting-of reference

?match[type]=sighting&match[sighting_of_ref]=<identifier>

For example, the filter,

?match[type]=sighting&match[sighting_of_ref]= indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7

will return the Sighting object shown in Figure 3, as well as all other sightings referencing the specified Indicator object in the **sighting_of_ref** property.


```
{
  "type": "sighting",
  "spec_version": "2.1",
  "id": "sighting--bfbc19db-ec35-4e45-beed-f8bde2a772fb",
```


[8] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_e2e1szrqfoan
[9] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_a795guqsap3r

```
    "created": "2016-04-06T20:06:37.000Z",
    "modified": "2016-04-06T20:06:37.000Z",
    "sighting_of_ref": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
    "where_sighted_refs": [
      "identity--311b2d2d-f010-4473-83ec-1edf84858f4c"
    ]
}
```


Figure 3: Sighting object

Output: Sightings of the Indicator object (indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7).

5.3 Internal References

In STIX, there are several objects that serve as containers for other objects (e.g., Grouping, Report, Bundle objects). This filter retrieves the specified type of such container objects filtering based on the **object_refs** property, which corresponds to the objects the container references.

5.3.1 Referenced objects

?match[type]=<string>&match[object_refs]=<identifier>

For example, the filter,

?match[type]=report&match[object_refs]= indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7,campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f

will return the Report object shown in Figure 4[10], as well as all other Report objects that reference the specified Indicator or Campaign objects in its **object_refs** property.[11]


```
{
  "type": "report",
  "spec_version": "2.1",
  "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
  "created_by_ref": "identity--311b2d2d-f010-4473-83ec-1edf84858f4c",
  "created": "2015-12-21T19:59:11.000Z",
  "modified": "2015-12-21T19:59:11.000Z",
  "name": "The Black Vine Cyberespionage Group",
  "description": "A simple report with an indicator and campaign",
  "report_types": [
    "campaign"
  ],
  "published": "2016-01-20T17:00:00Z",
  "object_refs": [
    "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
    "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
    "relationship--df7c87eb-75d2-4948-af81-9d49d246f301"
```


[10] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_n8bjzg1ysgdq
[11] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_pcpvfz4ik6d6

```
    ]
}
```

Figure 4: Report object

Output: Report objects that reference the Indicator (indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7) and/or Campaign (campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f) object.

5.4 Object Values

This filter retrieves cyber-observable objects based on the **value** property. The objects with a **value** property include Domain Name, Email Address, IPv4 Address, IPv6 Address, MAC Address, and URL.

5.4.1 Value property

?match[value]=<string>

For example, the filter,

?match[value]=bad-domain.com

will return a Domain Name object with a value of *bad-domain.com*, shown in Figure 5. [12]

```
{
  "id": "domain-name-- 3991931c-308f-533f-aa05-ac8d3fe79fac",
  "spec_version": "2.1",
  "type": "domain-name",
  "value": "bad-domain.com"
}
```

Figure 5: Domain Name object

Output: Domain Name object (domain-name--3991931c-308f-533f-aa05-ac8d3fe79fac).

5.5 Object Identifiers

This filter retrieves an object by its **id** property.

5.5.1 Id property

?match[id]=<identifier>

For example, the filter,

?match[id]=malware--496cac0a-77ea-4da0-b913-88e553483c8d

will return the Malware object shown in Figure 6.

```
{
 "type": "malware",
 "spec_version": "2.1",
 "id": "malware--496cac0a-77ea-4da0-b913-88e553483c8d",
 "created": "2017-03-10T07:31:09.000Z",
 "modified": "2017-03-10T07:31:09.000Z",
```

[12] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_prhhksbxbg87

```
"is_family": true,
"malware_types": [
  "bot"
],
"name": "Asprox"
}
```


Figure : Malware object

Output: Malware object (malware--496cac0a-77ea-4da0-b913-88e553483c8d).

6 Research Use Cases

The following examples describe use cases that enable an analyst to obtain a broader understanding (i.e. context) of the cyber threat intelligence shared by the AIS community.

6.1 Object Labels

The **labels** common property provides additional user-defined or trust-group defined context about a STIX object, other than that which can be expressed in other properties.[13] This filter retrieves objects based on keywords present in the **labels** property.

6.1.1 Label value

?match[labels]=<string>

For example, the filter,

?match[labels]=heartbleed

will return the object shown in Figure 5, as well as all other STIX objects that contain *heartbleed* in the labels property.


```
{
  "id": "vulnerability--ee916c28-c7a4-4d0d-ad56-a8d357f89fef",
  "spec_version": "2.1",
  "created": "2016-02-14T00:00:00.000Z",
  "modified": "2016-02-14T00:00:00.000Z",
  "type": "vulnerability",
  "name": "CVE-2014-0160",
  "description": "The (1) TLS...",
  "external_references": [
    {
      "source_name": "cve",
      "external_id": "CVE-2014-0160"
    }
```


[13] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_xzbicbtscatx

```
    ],
    "labels": ["heartbleed"]
}
```

Figure 6: Vulnerability object

Output: All objects that contain "heartbleed" as a label.

6.2 Identity Sectors

Relevant cyber threat intelligence can often be categorized by the sector that it impacts. This filter retrieves Identity objects associated with a specific sector by matching on the **sectors** property.[14]

6.2.1 Sectors

?match[type]=identity&match[sectors]=<open-vocab>

For example, the filter,

?match[type]=identity&match[sectors]=energy

will return the Identity object shown in Figure 6, as well as all other Identity objects that are indicated as being in the energy sector. The returned Identity objects can be used in follow-on filtering to, e.g., filter for all cyber threat intelligence created by organizations specified as being in the energy sector. See *Publisher Content section* for more information on how to write this follow-on filter using the information identified in the Identity object identifier (**id**) property.

```
{
    "type": "identity",
    "spec_version": "2.1",
    "name": "ACME Corp.",
    "identity_class": "organization",
    "created": "2017-06-01T00:00:00.000Z",
    "id": "identity--ede089d9-41f7-42a2-be58-4d6fb68204bd",
    "modified": "2017-06-01T00:00:00.000Z",
     "sectors": ["energy"]
}
```

Figure 7: Identity object

Output: All Identity objects from the energy sector.

6.3 Externally Referenced Identifiers

When the STIX object identifier (id) is not known, other information about the object, such as data in external registries (e.g., CVE, CAPEC, VERIS, ATT&CK, etc.), can be used for filtering. The following filters demonstrate how other information can be used to retrieve relevant STIX objects.

[14] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_wh296fiwpklp

6.3.1 External identifier

?match[external_id]=<string>

For example, the filter,

?match[external_id]=CVE-2016-1234

will return the Vulnerability object shown in Figure 7,[15] as well as all other objects that reference *CVE-2016-1234* in the external_id property.[16]


```
{
 "type": "vulnerability",
 "spec_version": "2.1",
 "id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",
 "created": "2016-05-12T08:17:27.000Z",
 "modified": "2016-05-12T08:17:27.000Z",
 "name": "CVE-2016-1234",
 "external_references": [
  {
   "source_name": "cve",
   "external_id": "CVE-2016-1234"
  }
 ]
}
```


Figure 8: Vulnerability object

Output: Objects that reference the CVE identifier (CVE-2016-1234) as an external identifier.

6.3.2 External reference source

?match[source_name]=<string>

For example, the filter,

?match[type]=attack-pattern&match[source_name]=mitre-attack

will return the Attack Pattern object shown in Figure 8,[17] as well as all other Attack Pattern objects that contain references to *mitre-attack* (MITRE ATT&CK) in the **source_name** property.[18]


```
{
   "type": "attack-pattern",
   "spec_version": "2.1",
   "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
   "created": "2017-05-31T21:30:54.661Z",
   "modified": "2017-05-31T21:30:54.661Z",
```


[15] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_q5ytzmajn6re
[16] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_72bcfr3t79jx
[17] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_axjijf603msy
[18] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_72bcfr3t79jx

```
  "id": "attack-pattern--02fefddc-fb1b-423f-a76b-7552dd211d4d",
  "name": "Bootkit",
  "external_references": [
    {
      "external_id": "T1067",
      "source_name": "mitre-attack",
      "url": "https://attack.mitre.org/techniques/T1067"
    }
  ]
}
```


Figure 9: Attack Pattern object

Output: Attack pattern objects that reference MITRE ATT&CK as the source in external references.

6.4 Traffic Light Protocol Markings

Traffic Light Protocol (TLP) markings are used to specify how cyber threat intelligence can be shared with other parties. These filters use the **object_marking_refs** property of a STIX object to return objects that are marked at a specific level.

Marking-definition objects may be filtered by UUID identifier or by shorthand keywords *white* (marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9), *green* (marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da), *amber* (marking-definition--f88d31f6-486f-44da-b317-01333bde0b82), and *red* (marking-definition--5e57c739-391a-4eb3-b6be-7d15ca92d5ed).[19,20,21] When using keywords, no values other than the keywords listed will return objects with these filters. The following filters demonstrate both ways of filtering on TLP markings.

6.4.1 Object marking identifier

?match[object_marking_refs]=<identifier>

For example, the filter,

?match[object_marking_refs]=marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9,marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da

will return the Indicator object shown in Figure 9, as well as all other objects marked with TLP:White (marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9) or TLP:Green (marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da).


```
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "created_by_ref": "identity--311b2d2d-f010-4473-83ec-1edf84858f4c",
  "created": "2017-01-01T00:00:01.000Z",
```


[19] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_yd3ar14ekwrs
[20] https://www.first.org/tlp/
[21] TLP Red submissions are not supported in AIS. As a result, any filter for TLP Red will not return any objects.

```
    "modified": "2017-01-01T00:00:01.000Z",
    "indicator_types": [
      "malicious-activity"
    ],
    "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
    "pattern_type": "stix",
    "valid_from": "1970-01-01T00:00:01Z",
    "object_marking_refs": [
      "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
    ]
}
```


Figure 10: Indicator object (TLP: White)

Output: All objects marked TLP:White or TLP:Green.

6.4.2 Marking keywords

?match[tlp]=<string>

For example, the filter,

?match[tlp]=white,green

will return the Indicator object in Figure 9, as well as all other objects marked TLP:White (marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9) or TLP:Green (marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da).

Output: All objects marked TLP:White or TLP:Green.

Similarly, the filter,

?match[type]=indicator&match[tlp]=amber

will return the Indicator object shown in Figure 11, as well as all other Indicator objects marked TLP:Amber (marking-definition--f88d31f6-486f-44da-b317-01333bde0b82).


```
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "created": "2017-01-01T00:00:01.000Z",
  "modified": "2017-01-01T00:00:01.000Z",
  "indicator_types": [
    "malicious-activity"
  ],
  "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
  "pattern_type": "stix",
  "valid_from": "1970-01-01T00:00:01Z",
```

```
  "object_marking_refs": [
    "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82"
  ],
  "confidence": 91
}
```


Figure 11: Indicator object (TLP: Amber)

Output: All Indicator objects marked TLP:Amber.

6.5 STIX Version

This filter matches against the **spec_version** property, which denotes the version of the STIX specification used to represent an object.

6.5.1 Spec version

?match[spec_version]=<keyword>

For example, the filter,

?match[spec_version]=2.1

Will return the object shown in Figure 12, as well as all objects defined according to the STIX 2.1 specification.


```
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "created": "2017-01-01T00:00:01.000Z",
  "modified": "2017-01-01T00:00:01.000Z",
  "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
  "pattern_type": "stix",
  "valid_from": "1970-01-01T00:00:01Z",
}
```


Figure 12: Indicator object (spec version 2.1)

Output: All objects defined according to the STIX 2.1 specification.

7 Trust Use Cases

The following examples support use cases that an analyst might use to evaluate the relevance of AIS data. For example, trust use cases relate to content created by specific organizations that are trusted by the analyst, as well as confidence scores and opinion values.

7.1 Opinion

This filter matches against the **opinion** property of an Opinion object[22] to retrieve Opinion objects with specific

[22] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_ht1vtzfbtzda

opinion values. This property can only contain the keywords *strongly-disagree*, *disagree*, *neutral*, *agree*, and *strongly-agree*. Any other values given for this filter will not return objects.

7.1.1 Opinion property

?match[type]=opinion&match[opinion]=<keyword>

For example, the filter,

?match[type]=opinion&match[opinion]=strongly-agree

will return the CISA-created Opinion object shown in Figure 13, as well as all other Opinion objects with an opinion value of *strongly-agree*.


```
{
 "type": "opinion",
 "spec_version": "2.1",
 "id": "opinion--c18c72f9-abdd-490a-9781-aaf3b9c50eaa",
 "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
 "created": "2020-10-30T12:17:27.000Z",
 "modified": "2020-10-30T12:17:27.000Z",
 "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
 ],
 "object_refs": ["indicator--e9455434-be0c-4c14-a5f4-a7cd51d547a3"],
 "opinion": "strongly-agree",
 "explanation": " Confirmed; likely malicious (if marked or otherwise evaluated
                  as malicious-activity) or benign (if marked as benign);
                  consistent with other information on the subject known to the
                  opinion author. Please see the AIS Scoring
                  Framework Used for Indicator Enrichment at
                  https://www.cisa.gov/publication/automated-
                  indicator-sharing-ais-documentation for more information on
                  how the opinion is derived.",
 "external_references": [
  {
     "source_name": "AIS Scoring Framework Used for Indicator Enrichment",
     "description": "This reference provides more information about the AIS
                       Scoring Framework and how the opinion is derived.",
     "url": "https://www.cisa.gov/publication/automated-indicator-sharing-ais-
             documentation"
  }
 ]
}
```


Figure 13: Opinion object (strongly agree)

Output: All Opinion objects with an opinion value of strongly-agree.

7.2 Confidence

These filters match against the **confidence** property of a STIX object, which specifies the confidence the creator has in the correctness of their data.[23] This value must be an integer from 0 to 100, so only filters that use such values will return objects. The following filters demonstrate how the confidence score can be used to return relevant STIX objects.

7.2.1 Single confidence value

?match[confidence]=<integer>

For example, the filter,

?match[confidence]=90

will return the Course of Action object shown in Figure 14,[24] as well as all other objects that have a confidence score of *90*.


```
{
  "type": "course-of-action",
  "spec_version": "2.1",
  "id": "course-of-action--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "created": "2016-04-06T20:03:48.000Z",
  "modified": "2016-04-06T20:03:48.000Z",
  "name": "Add TCP port 80 Filter Rule to the existing Block UDP 1434 Filter",
  "description": "This is how to add a filter rule to block inbound access to TCP
   port 80 to the existing UDP 1434 filter ...",
  "confidence": 90
}
```


Figure 14: Course of Action object (confidence 90)

Output: All objects with a confidence score of 90.

7.2.2 Multiple confidence values

?match[confidence]=<integer>,<integer>,<integer>

For example, the filter,

?match[type]=indicator&match[confidence]=90,91,92,93,94,95,96,97,98,99,100

will return the Indicator object shown in Figure 15, as well as all other Indicator objects that have a confidence score of *90 or above*.


```
{
  "type": "indicator",
  "spec_version": "2.1",
```


[23] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_xzbicbtscatx
[24] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_a925mpw39txn

```
  "id": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
  "created": "2017-01-01T00:00:01.000Z",
  "modified": "2017-01-01T00:00:01.000Z",
  "indicator_types": [
    "malicious-activity"
  ],
  "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
  "pattern_type": "stix",
  "valid_from": "1970-01-01T00:00:01Z",
  "confidence": 91
}
```


Figure 15: Indicator object (confidence 91)

Output: All Indicator objects with a confidence score of 90 or above.

7.3 Publisher Content

This filter retrieves all STIX objects created by a particular entity. The **created_by_ref** property of a STIX object points to the producer Identity object that represents the entity responsible for creating the STIX object.[25] Filters may be created against this property to get all STIX objects created by a particular entity. For example, matching on the identifier, *identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01*, will retrieve content created by CISA.

7.3.1 Created by reference

?match[created_by_ref]=<identifier>

For example, the filter,

?match[created_by_ref]=identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01

will return the Identity object shown in Figure 16, as well as all objects created by CISA (identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01).


```
{
  "type": "identity",
  "spec_version": "2.1",
  "id": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
  "created": "2021-01-01T00:00:01.000Z",
  "modified": "2021-01-01T00:00:01.000Z",
  "name": "Cybersecurity and Infrastructure Security Agency",
  "description": "The United States Cybersecurity and Infrastructure Security
   Agency (CISA) is the Nation's risk advisor, working with partners to defend
```


[25] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_xzbicbtscatx

```
    against today's threats and collaborating to build more secure and resilient
    infrastructure for the future.",
   "identity_class": "organization",
   "sectors": ["government-national"],
   "contact_information": "cyberservices@cisa.dhs.gov"
}
```


Figure 16: Indicator object

Output: All objects created by CISA.

7.4 Valid/Active Indicators

This filter retrieves all Indicator objects that are valid on or after a given date. Indicator objects in STIX may have a lifespan associated with them that specifies when an Indicator object is considered valid and when it is considered no longer valid. This helps identify Indicator objects that are still relevant (i.e., specified timestamp is greater than or equal to **valid_from**, less than **valid_until**, and not revoked).

7.4.1 Validity dates

?match[valid_on_after]=<timestamp>

For example, the filter,

?match[valid_on_after]=2020-05-25T01:01:01.000Z

will return the Indicator object shown in in Figure 17, as well as all other Indicator objects that are valid on or after the specified timestamp *2020-05-25T01:01:01.000Z*.


```
{
   "type": "indicator",
   "spec_version": "2.1",
   "id": "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
   "created": "2021-01-01T00:00:01.000Z",
   "modified": "2021-01-01T00:00:01.000Z",
   "indicator_types": [
      "malicious-activity"
   ],
   "pattern": "[file:hashes.MD5 = 'd41d8cd98f00b204e9800998ecf8427e']",
   "pattern_type": "stix",
   "valid_from": "2021-04-01T00:00:01Z",
   "confidence": 91
}
```


Figure 17: Indicator object

Output: All Indicator objects that are valid on or after May 25, 2020, 01:01:01.

8 Advanced Use Cases

The following use cases are more advanced than those in the previous sections. Some span multiple use case categories.

8.1 Opinion with Specific Opinion and Sector Values

Categories: Trust, Research

This set of filters retrieves all Indicator objects, valid on or after a specified date, that are both created by entities in specific sectors and for which CISA has an Opinion object with an **opinion** property value of *neutral*, *agree*, or *strongly-agree*. The filter requires three steps:

1. Find Identity objects with specific **sector** property value(s):

   ?match[type]=identity&match[sectors]=<string>

2. Find Indicator objects where the created_by_ref property matches one of the Identity objects found in Step 1 and that are valid on or after (**valid_on_after**) a specified timestamp:

   ?match[type]=indicator&match[created_by_ref]=<identifier>&match[valid_on_after]=<timestamp>

3. Find CISA Opinion objects (**created_by_ref** property is *identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01*) where the **opinion** property has value *neutral, agree,* or *strongly-agree* and the **object_refs** property matches the identifier of one of the Indicator objects from Step 2.

   ?match[type]=opinion&match[created_by_ref]=identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01&match[opinion]=neutral,agree,strongly-agree&match[object_refs]=<identifier>

8.1.1 Step 1: Identity objects are found with energy, utilities, government-national sector property value(s).

The filter,

?match[type]=identity&match[sectors]=energy,utilities,government-national

will return all Identity objects corresponding to organizations from the energy, utilities, and/or national government sectors. For example, the Identity object in Figure 18 would be returned.


```
{
  "type": "identity",
  "spec_version": "2.1",
  "name": "PowerCo",
  "identity_class": "organization",
  "created": "2017-06-01T00:00:00.000Z",
  "id": "identity--9584ffbf-b475-2323-be09-00304bded523",
  "modified": "2021-06-21T00:00:00.000Z",
  "sectors": ["energy"]
}
```


Figure 18: Identity object (energy sector)

8.1.2 Step 2: Indicator objects are found where the created_by_ref property matches the Identity objects found in Step 1 (identity–9584ffbf-b475-2323-be09-00304bded523) and where the Indicator is valid on or after 2020-06-01T00:00:01Z.

The filter,

?match[type]=indicator&match[created_by_ref]=identity--9584ffbf-b475-2323-be09-00304bded523&match[valid_on_after]=2020-06-01T00:00:01Z

can be developed using the returned Identity objects (e.g., the Identity object in Figure 18) to return all Indicator objects created by that Identity object that are valid on or after the specified timestamp. For example, the Indicator object shown in Figure 19 would be returned.


```
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--fbf92301-63af-4eb9-a001-f9090495034f",
  "created_by_ref": "identity--9584ffbf-b475-2323-be09-00304bded523",
  "created": "2021-01-11T00:00:01.000Z",
  "modified": "2021-01-11T00:00:01.000Z",
  "indicator_types": [
    "malicious-activity"
  ],
  "pattern": "[file:hashes.MD5 = '953fbf398f00b20492933334ecf41a7e']",
  "pattern_type": "stix",
  "valid_from": "2020-07-31T00:00:01Z",
}
```


Figure 19: Indicator object

8.1.3 Step 3: CISA Opinion objects are found where the opinion property has value neutral, agree, or strongly-agree and the object_refs property matches one of the Indicator objects from Step 2 (indicator–fbf92301-63af-4eb9-a001-f9090495034f).

The filter,

?match[type]=opinion&match[created_by_ref]=identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01&match[opinion]=neutral,agree,strongly-agree&match[object_refs]=indicator–fbf92301-63af-4eb9-a001-f9090495034f

can be developed using the returned Indicator objects (e.g., the Indicator object in Figure 19) to return all CISA Opinion objects with an opinion value of *neutral*, *agree*, or *strongly-agree* that reference that returned Indicator object. For example, the Opinion object in Figure 20 would be returned.


```
{
 "type": "opinion",
 "spec_version": "2.1",
```

```
  "id": "opinion--8456fbcd-0505-3bbc-29405bfa5546",
  "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
  "created": "2020-10-30T12:17:27.000Z",
  "modified": "2020-10-30T12:17:27.000Z",
  "object_refs": ["indicator--fbf92301-63af-4eb9-a001-f9090495034f"],
  "opinion": "agree",
  "explanation": "Confirmed; consistent with other information...",
}
```


Figure 20: Opinion object (agree)

Output (for the full set of filters): CISA Opinion object with an opinion value of neutral, agree, or strongly-agree referring to Indicator objects valid after 2020-06-01T00:00:01Z and created by an entity in the energy, utilities, government-national sectors.

8.2 Content from a Specific Organization with a Specific TLP Marking

Category: Trust, Research

This filter matches against both the **created_by_ref** and **object_marking_refs** properties to return objects created by a specific organization with specific TLP markings. The filter requires one step with two match parameters:

1. Find objects with specific **created_by_ref** and **object_marking_refs** properties:

   ?match[created_by_ref]=<identifier>&match[object_marking_ref]=<identifier>

For example, the filter,

?match[created_by_ref]=identity--311b2d2d-f010-4473-83ec-1edf84858f4c&match[object_marking_refs]=marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9,marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da

will return all objects created by the specific organization (identity--311b2d2d-f010-4473-83ec-1edf84858f4c) with TLP:White (marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9) or TLP:Green (marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da) markings (including the Report object shown in Figure 21, as well as any other objects that meet these parameters).


```
{
  "type": "report",
  "spec_version": "2.1",
  "id": "report--84e4d88f-44ea-4bcd-bbf3-b2c1c320bcb3",
  "created_by_ref": "identity--311b2d2d-f010-4473-83ec-1edf84858f4c",
  "created": "2015-12-21T19:59:11.000Z",
  "modified": "2015-12-21T19:59:11.000Z",
  "name": "The Black Vine Cyberespionage Group",
  "description": "A simple report with an indicator and campaign",
  "report_types": [
```

```
        "campaign"
      ],
      "published": "2016-01-20T17:00:00Z",
      "object_refs": [
        "indicator--a740531e-63ff-4e49-a9e1-a0a3eed0e3e7",
        "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
        "relationship--df7c87eb-75d2-4948-af81-9d49d246f301"
      ],
      "object_marking_refs": [
        "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
      ]
    }
```


Figure 21: Report object that includes an indicator and campaign

Output: All objects created by the identified organization (identity--311b2d2d-f010-4473-83ec-1edf84858f4c), marked TLP:White or TLP:Green.

2. As a second example, the filter,

   ?match[type]=report&match[created_by_ref]=identity--311b2d2d-f010-4473-83ec-1edf84858f4c&match[object_marking_refs]=marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9,marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da

will return the Report object shown in Figure 21, as well as all other *Report* objects created by the specific organization and marked TLP:White (marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9) or TLP:Green (marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da).

Output: All Report objects created by the organization (identity--311b2d2d-f010-4473-83ec-1edf84858f4c), marked TLP:White or TLP:Green.

8.3 Observed Data That References a Particular Object

Category: Hunt

This set of filters uses auxiliary information to retrieve Observed Data objects referencing a particular object when its STIX object identifier is not initially known. The following filters demonstrate how relevant information can be used to retrieve Observed Data objects using auxiliary information. The filter requires two steps:

1. Find object identifiers with matches to known auxiliary information;

   ?match[type]=<string>&match[*field*]=<string>

2. Find Observed Data objects that reference the objects found in Step 1.

   ?match[type]=observed-data&match[object_refs]=<identifier>

8.3.1 Step 1: IPv4 Address objects are found with 1.2.3.4 or 15.16.17.18 value property values.

The filter,

?match[type]=ipv4-addr&match[value]=1.2.3.4,15.16.17.18

will return all IPv4 Address objects with a value of *1.2.3.4* or *15.16.17.18*, including the two IPv4 Address objects shown in Figure 22. [26]


```
{
  "id": "ipv4-addr--b4127704-cf21-56bb-885a-d481ca0b147e",
  "spec_version": "2.1",
  "type": "ipv4-addr",
  "value": "1.2.3.4"
}
{
  "id": "ipv4-addr--a9cfdbf6-1e9a-57c3-b912-35c4b210e754",
  "spec_version": "2.1",
  "type": "ipv4-addr",
  "value": "15.16.17.18"
}
```


Figure 22: IPv4 Address objects

8.3.2 Step 2: Observed Data objects are found that reference the IPV4 Address objects found in Step 1 (ipv4-addr–b4127704-cf21-56bb-885a-d481ca0b147e and ipv4-addr–a9cfdbf6-1e9a-57c3-b912-35c4b210e754).

The filter,

?match[type]=observed-data&match[object_refs]= ipv4-addr--b4127704-cf21-56bb-885a-d481ca0b147e,ipv4-addr--a9cfdbf6-1e9a-57c3-b912-35c4b210e754

uses object identifiers and the **object_refs** property to return all Observed Data objects referencing one or both of the IPv4 Address objects.[27] For example, the two Observed Data objects in Figure 23 would be returned.


```
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--b67d30ff-02ac-498a-92f9-32f845f448cf",
  "created_by_ref": "identity--311b2d2d-f010-4473-83ec-1edf84858f4c",
  "created": "2016-04-06T19:58:16.000Z",
  "modified": "2016-04-06T19:58:16.000Z",
  "first_observed": "2015-12-21T19:00:00Z",
  "last_observed": "2015-12-21T19:00:00Z",
  "number_observed": 50,
  "object_refs": [
    "ipv4-addr--b4127704-cf21-56bb-885a-d481ca0b147e"
  ]
```


[26] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_ki1ufj1ku8s0
[27] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_p49j1fwoxldc

```
}
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--7e406b59-c860-5deb-b331-a1dab054732b",
  "created_by_ref": "identity--311b2d2d-f010-4473-83ec-1edf84858f4c",
  "created": "2019-03-16T09:00:10.000Z",
  "modified": "2019-03-16T09:00:10.000Z",
  "first_observed": "2017-11-20T12:00:00Z",
  "last_observed": "2017-11-20T12:00:00Z",
  "number_observed": 76,
  "object_refs": [
    "ipv4-addr--a9cfdbf6-1e9a-57c3-b912-35c4b210e754"
  ]
}
```


Figure 23: Observed Data objects that point to IPv4 addresses

Output (for the full set of filters): Observed Data objects that reference the IPv4 address objects (ipv4-addr–b4127704-cf21-56bb-885a-d481ca0b147e,ipv4-addr–a9cfdbf6-1e9a-57c3-b912-35c4b210e754).

8.4 Object Referenced by Opinion

Category: Trust

This set of filters retrieves objects that are referenced in Opinion objects created by a specific entity with specific values in the **opinion** property.[28] The filter requires two steps:

1. Find Opinion objects with specific **created_by_ref** and **opinion** properties:

   ?match[type]=opinion&match[created_by_ref]=<identifier>&match[opinion]=<keyword>

2. Find objects that are referenced in the **object_refs** property of the Opinion objects returned in Step 1.

   ?match[id]=<identifier>

8.4.1 Step 1: Opinion objects are found that are created by CISA (identity–b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01) with an opinion value of strongly-agree.

The filter:

?match[type]=opinion&match[created_by_ref]=identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01&match[opinion]=strongly-agree

will return the Opinion object shown in Figure 24, as well as all other Opinion objects created by CISA with an opinion value of *strongly-agree*.


```
{
 "type": "opinion",
```


[28] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_ht1vtzfbtzda

```
 "spec_version": "2.1",
 "id": "opinion--2a59fae8-93f4-5405-9e44-c4caefff468f",
"created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
 "created": "2021-11-19T12:00:00.000Z",
 "modified": "2021-11-19T12:00:00.000Z",
 "object_refs": ["indicator--e9455434-be0c-4c14-a5f4-a7cd51d547a3"],
"opinion": "strongly-agree",
 "explanation": "Confirmed by multiple sources",
}
```


Figure 24: Opinion object

8.4.2 Step 2: Objects are found that are referenced in the object_refs property of the Opinion objects returned in Step 1 (indicator–e9455434-be0c-4c14-a5f4-a7cd51d547a3).

The filter:

?match[id]=indicator--e9455434-be0c-4c14-a5f4-a7cd51d547a3

will return the Indicator object shown in Figure 25, which is the Indicator referenced in the **object_refs** property of the Opinion object shown in Figure 24.


```
{
 "type": "indicator",
 "spec_version": "2.1",
 "id": "indicator--e9455434-be0c-4c14-a5f4-a7cd51d547a3",
 "created_by_ref": "identity--a7163454-a268-494b-ba07-557023d88014",
 "created": "2020-10-30T08:17:27.000Z",
 "modified": "2020-10-30T08:17:27.000Z",
 "object_marking_refs": [
    "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"],
 "name": "Malicious IP Address",
 "description": "This IP address is associated with known malicious activity.",
 "indicator_types": ["malicious-activity"],
 "pattern": "[ipv4-addr:value = '198.51.100.3']",
 "pattern_type": "stix",
 "valid_from": "2020-10-30T00:00:00Z",
 "confidence": 75
}
```


Figure 25: Indicator object

Output (for the full set of filters): Indicator objects referenced in an Opinion object created by CISA with an opinion value of strongly-agree.

9 Appendix A – Acronyms

Acronyms are provided below.

Acronym	Definition
AIS	Automated Indicator Sharing
CISA	Cybersecurity and Infrastructure Security Agency
CTI	Cyber Threat Indicator
CTIS	Cyber Threat Information Sharing
DM	Defensive Measure
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information