STIX Opinion Object

"Hey, I don't agree with that!"

What is it?

The Opinion object is an object that allows the creator of the Opinion object to agree/disagree with any other STIX Data Object or STIX Relationship Object. It will allow an Organization to disagree with a relationship between a Threat Actor and a Campaign for example, or agree with the contents of an Course of Action.

This is the first step towards consumers being able to crowdsource the opinion of the community, which will help newcomers to the threat intelligence sharing groups better understand which threats have a high degree of community agreement and which are contentious.

Why do we need it?

There is currently no direct way to agree or disagree with someone else's assertion.

This single fact makes it difficult for consumers to know which threat intelligence is 'commonly agreed' as being correct within a community, and which threat intelligence is actually something that only a few Organizations believe.

This in turn makes it difficult for consumers to determine which threat intelligence they should believe out of all the threat intelligence they have available.

As an example, imagine that Org A released a relationship object between the CrystalFlower threat actor and the FlowerTank Campaign to a threat sharing community, and imagine that most of the community actually disagreed with this assertion. Org B, as a recipient of this assertion, would have no idea that the most of the community disagreed with this relationship, and it could assume that the relationship object is really good, when in fact the community as a whole thinks it is a bad assertion.

What if community members had the ability to agree or disagree with another organization's assertion? If they were able to, the situation above would look very different.

To revisit the previous example, if the Opinion object existed, as soon as Org A released its relationship object, the other organizations in the threat sharing community would be able to publish their own Opinion objects disagreeing with the relationship. Org B would be able to now see that many organizations disagreed with the assertion that Org A made, and Org B will now have a much better picture of how people on the community feel.

In short - the Opinion object will reduce the likelihood that recipients treat the threat intelligence they receive as the truth.

How would it work?

I propose that we add one new STIX Data Object called the Opinion object. The Opinion object would have one embedded **object_ref** field that would specify the single STIX object (either a SDO or SRO) that the opinion is regarding.

What benefits would it provide?

An Opinion object would provide the following benefits:

- It will allow community members to better understand which threat intelligence is highly contentious, and which threat intelligence is commonly believed.
- It provides more information for Threat Intelligence Platforms to automatically filter out untrusted threat intelligence
- It will reduce the likelihood of recipients using highly 'untrusted' threat intel accidentally.
- **It aids consensus forming across a community**
- It allows consumers to develop an understanding over time of which threat intelligence sources are highly contentious and which are commonly agreed with, who they should ignore and who they should prioritize.

STIX object proposal

Opinion

Type Name: `opinion`	**Status:** Proposal **MVP**: Yes

The Opinion object is used to convey an opinion about another creator's STIX object. It will allow an organization to agree or disagree with another organization's assertions, and ultimately will enable consumers to collect and understand the collective opinions of the community about the quality of the threat intelligence they have received.

It allows consumers to develop an understanding over time of which threat intelligence sources are highly contentious and which are commonly agreed with, who they should ignore and who they should prioritize.

This is the first step towards consumers being able to crowdsource the opinion of the community, which will help newcomers to the threat intelligence sharing groups better understand which threats have a high degree of agreement and which are contentious.

Properties

STIX TLO Common Properties		
type, id, created_by_ref, revision, created_time, modified_time, revoked, `revision_comment`, `object_markings_refs`, `granular_markings`		
Property Name	**Type**	**Description**
type (required)	`string`	The value of this field **MUST** be `opinion`
description (optional)	`string`	A description that provides the recipient with reasoning to back up the opinion identified in this Opinion object.

object_ref(required)	`identifier`	The **id** of the object that the Opinion refers to. This **id** can be any other STIX TLO except another Opinion object.
opinion(required)	`list` of type `controlled-vocab`	The opinion that the producer has about the object listed in the object_ref field. This is one of the following options: • "strongly-agree" • "agree" • "neutral" • "disagree" • "strongly-disagree" • "no-opinion"

Relationships

The Opinion object is a STIX Data Object but **MUST NOT** have any SRO-based relationships to it or from it. It **MAY** have a direct embedded relationship to only one STIX Data Object or STIX Relationship Object..

Example

```
{
  "type": "opinion",
  "id": "opinion--b01efc25-77b4-4003-b18b-f6e24b5cd9f7",
  "spec_version": "2.1",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "description": "This doesn't seem like it is feasible. We've seen how PandaCat has attacked Spanish infrastructure over the last 3 years, so this change in targeting seems too great to be viable. The methods used are more commonly associated with the FlameDragonCrew.",
  "object_ref": "relationship--16d2358f-3b0d-4c88-b047-0da2f7ed4471",
  "opinion": "disagree"
}
```