STIX Question and Answer

"Ask everyone in the community a question"

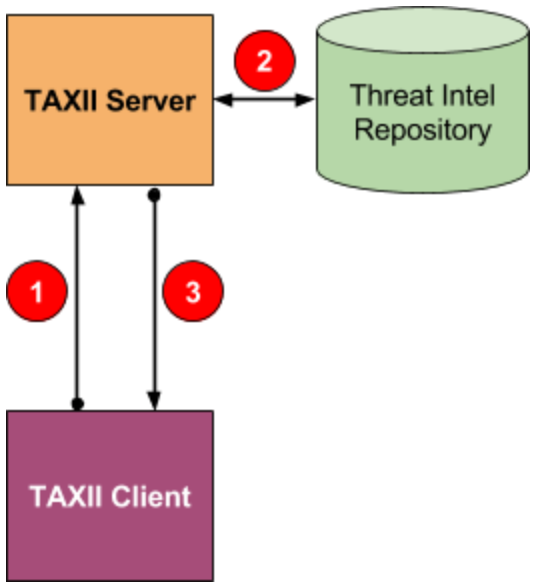
What is it?

In my discussion with colleagues, community groups and customers, one of the question's I keep getting asked about STIX is **"Can I ask the community I'm in if anyone has information about a particular IP address?**". At present my answer is …."Well, actually no. Not at present. You can only see what others have sent out."

If we implemented this proposal, people would be able to ask others for intel about things like IP addresses, file hashes and domain names.

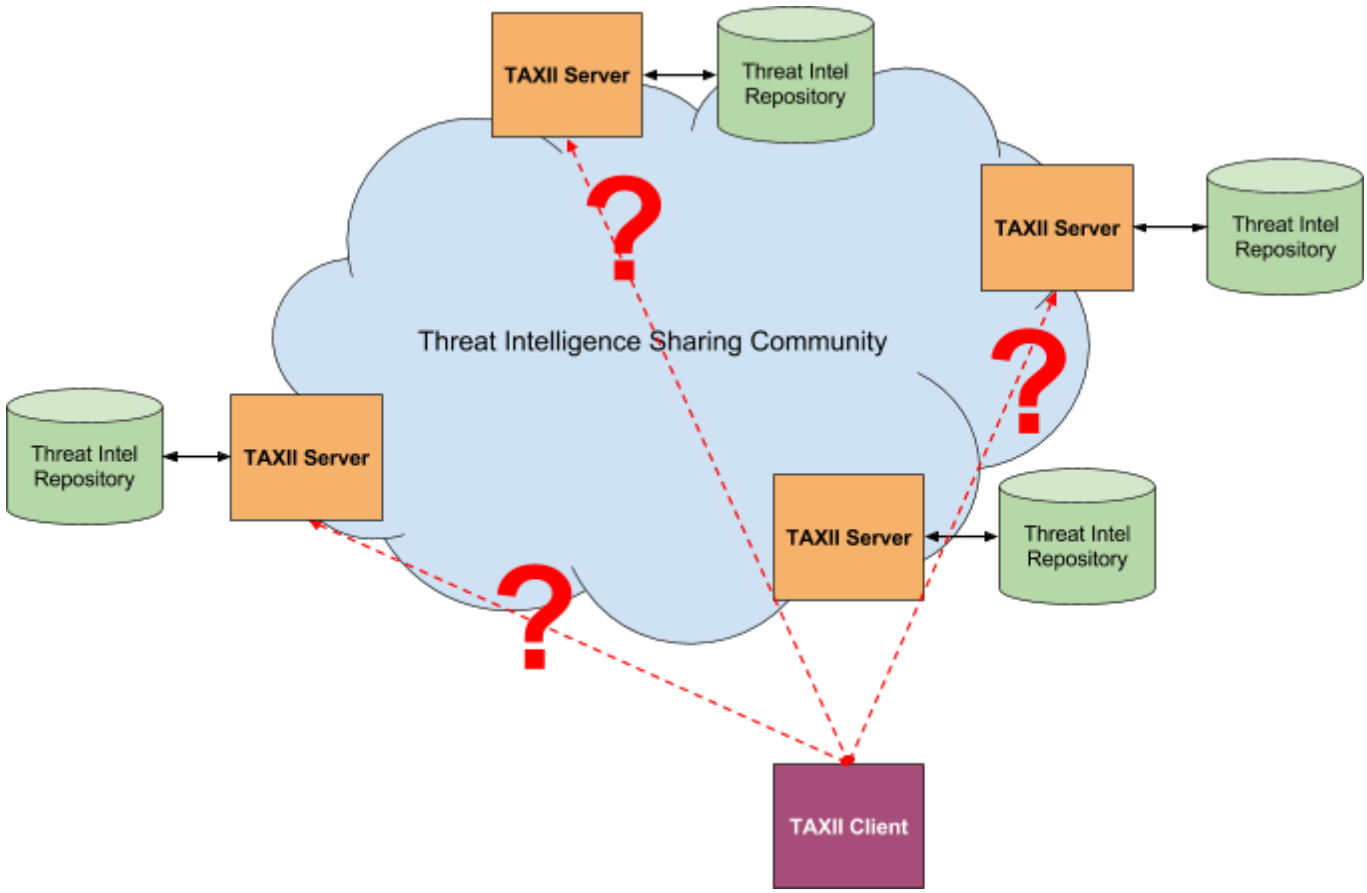
Why do we need it?

Within TAXII 2.0, we have the ability to ask our local server questions using the local TAXII server query functionality. This allows us to ask the local TAXII Server to which we have connected for information about something we wish to know about?



This is fine if we have a single TIP, and it contains all the information we need to know about.

But what if we are part of a larger threat intelligence sharing community? How do we ask everyone in the community if they know about an IP address?



This problem ***could*** be solved by making every single member of a threat intelligence community create a connection to every other member of the threat intelligence community, and they ***could*** then query every single other member of the threat intelligence community when they have a question they want answered, but that potential solution has the following problems:

- It scales badly. Larger trust groups are over 400 people in size, with over 300 organizations. It would be a huge amount of work to create and maintain links to all these different TAXII Servers.
- Whenever you want to ask a question, you need to cycle through every TAXII Server. This will take a large amount of time and create a large number of connections.
- Each organization would require a username and password combination on each TAXII server within the trustgroup. This is a problem to maintain.

A far *better* solution is to provide the ability for an organization to broadcast their question to the group, and to request that people provide answers back.

That is exactly what this proposal attempts to define.

What's it got to do with STIX?

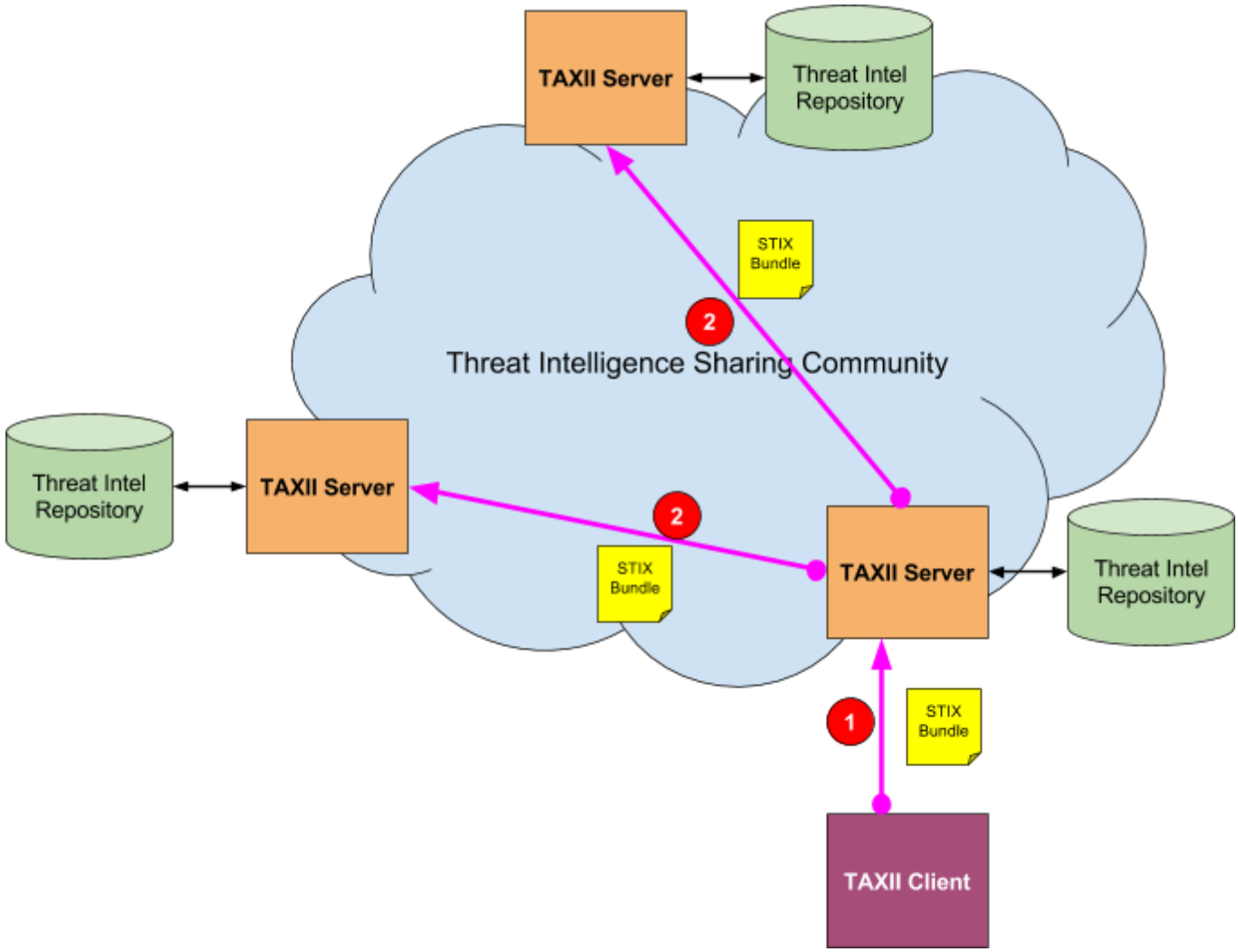
Good question! This seems like a TAXII problem….

Well I believe this is an issue that STIX is best placed to solve, and this has to do with the line I mentioned at the end of the previous section:

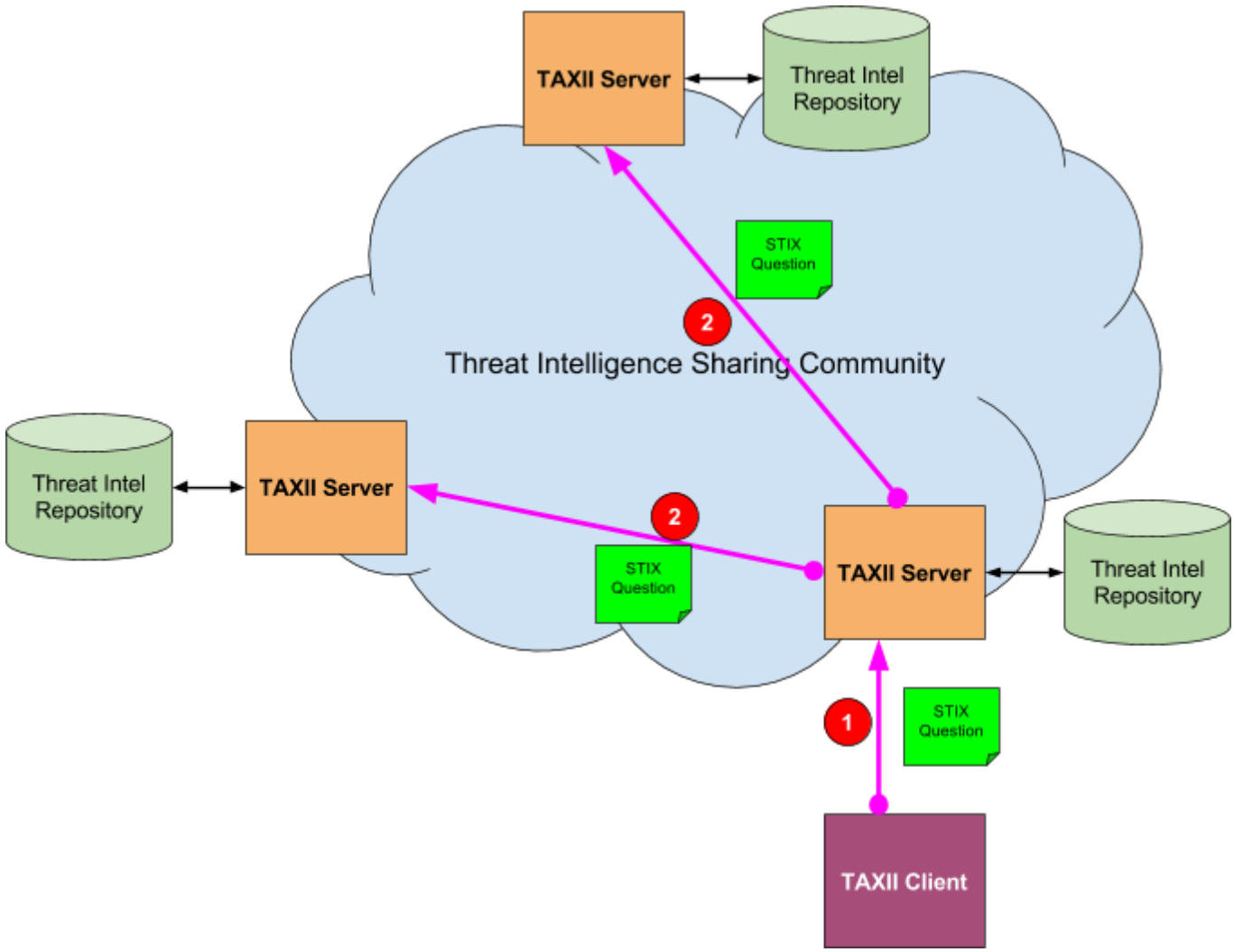
A far *better* solution is to provide the ability for an organization to broadcast their question to the group, and to request that people provide answers back.

We need a way of broadcasting the question to everyone on a trustgroup, and allowing them to respond back. Initially it seems like we need a TAXII enhancement to allow that to happen, but I would argue that we already have the functionality we require.

TAXII **already broadcasts STIX intelligence assertions** to community members as STIX bundles:



Why not just treat the questions and answers as broadcast STIX objects too? Then the existing TAXII communication mechanism will be able to treat STIX Questions and STIX Answers exactly the same as the current STIX Bundles, and there is minimal extra complexity!



This then becomes a STIX change, not a TAXII change.

How would it work?

I propose that we add two new STIX message containers as alternatives to the STIX Bundle message container. Those two message containers are:

1. STIX Question
2. STIX Answer

Draft normative text for both the STIX Question and STIX Answer objects are listed at the end of this document.

The important points are:

- A STIX question object will allow an Organization to broadcast a question to all the community members.

- If any one of the organization's within the threat intelligence sharing community have some threat intelligence that helps answer the STIX question and if the organization wishes to share the information they have (Answering a STIX Question is completely optional) then the replying organization can use a STIX Answer to reply to the STIX Question with the answer.

- STIX Answers are broadcasts too. This means that it uses the same TAXII sharing mechanism that exists today. It also means that all members of the threat intelligence sharing community gets

to see the same answers, allowing each community member to update their threat intelligence repository with the information.

- STIX Questions and STIX Answers would become additional STIX message types, similar to the STIX Bundle message type. They would be transported by TAXII in exactly the same way as STIX Bundles are now.

What benefits would it provide?

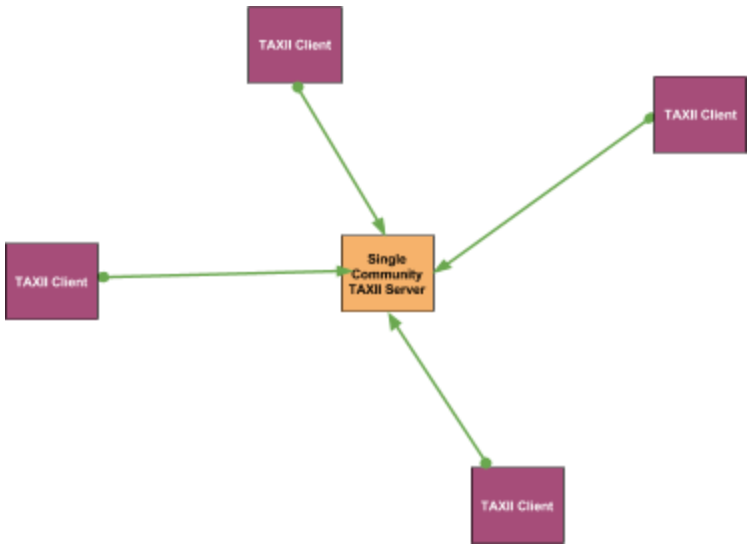
STIX Question and Answers provide the following benefits:

- It allows community members to ask questions about particular threat intelligence they wish to know more about. This currently happens over email - we would allow this to happen in a automated, structured way, and would allow the information to automatically be ingested into their organization's TIP.
- It speeds up the answering of questions. As mentioned above, this question/response process already happens over encrypted email and in secured forums. We would just be allowing it to happen at scale, automatically and much faster than currently happens.
- It allows the questions and answers to tie directly to STIX objects. As the questions and answers are in STIX, when an answer is received, it can easily be ingested into the TIP. It eliminates the current manual process that all recipients need to do at present, which is manually transpose all answers into STIX.
- The questions that people are asking will be able to be used as threat intelligence in its own right. Let's say that Org A asks about a particular file hash, and no-one has any threat intelligence about it. Lets then say that a few days later Org B finds that file, they will be able to know that the file MAY be suspicious, because Org A thought that it was suspicious enough to ask a STIX Question to the community. This could help Org B perform additional testing on the file, or maybe quarantine the file for manual review.
- The changes are only required within STIX. Because the Question and Answer objects are STIX, and they are shared using existing TAXII connectivity, it's simpler to implement. They are simply additional STIX objects.
- Because they are within STIX we can even make them optional STIX objects. If a TIP doesn't want to implement the STIX Question or STIX Answer objects, they won't have to (although they would lose a lot of functionality if they don't!)

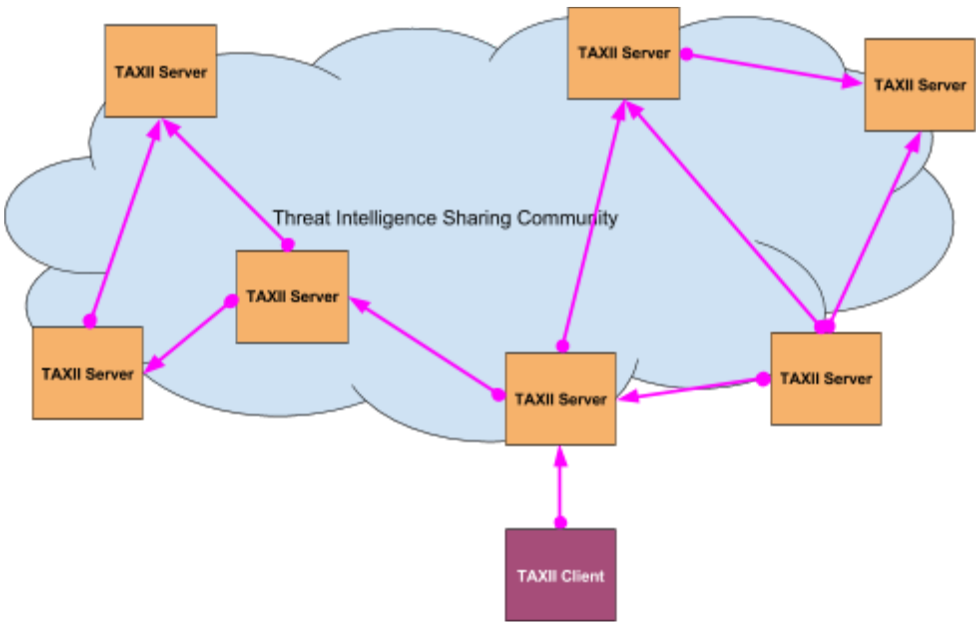
Why not just enhance TAXII query?

TAXII query is about querying a single TAXII server for information that it has. In this instance we want ALL community members on all TAXII servers that are part of the community to be see the STIX question, and to be able to provide a STIX Answer if they want.

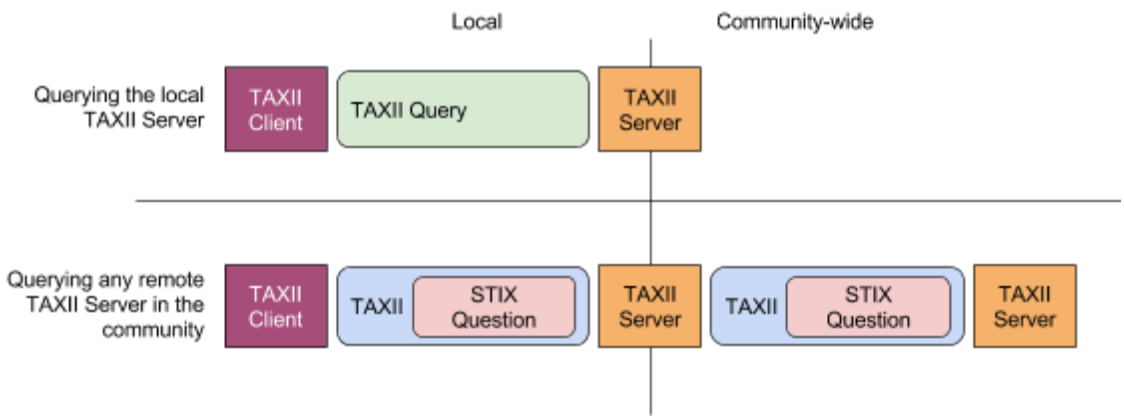
TAXII query could only work if all TAXII Communities look like this:



The issue with this is that not all communities operate as hub and spoke. We need a way that will support communities that are mesh in style, or made up of a bunch of partial connections connections that have grown organically over time - where multiple different TAXII servers are part of the TAXII community, all connected in various ways. They look more like this:



STIX Question objects and STIX Answer objects would work in the above scenario, and they would also allow each protocol to take care of what it's best at:



STIX object proposals

STIX Question

Type Name: `question`	**Status:** Proposal **STIX 2.1**: Undecided

The STIX Question message type is used to allow a member of a threat intelligence community (the requestor) to request information from the other members of the group (responders). A STIX Question MAY have one or more related STIX Answer objects associated with it, if any of the community members choose to answer question posed within the STIX Question object.

Answering a STIX Question by creating and issuing a related STIX Answer is optional.

The STIX Question is not a STIX Data Object or a STIX Relationship Object, so it does not have any of the Common Properties other than the **type, id,** and **created_by_ref** fields. The STIX Question has a limited lifespan, and should be considered transient in nature, and implementations should not assume that other implementations will treat it as a persistent object.

The JSON MTI serialization uses the JSON object type <TODO: add reference> when representing `question`.

5.1. Properties

Property Name	Type	Description
type (required)	`string`	The value of this field **MUST** be `question`
id (required)	`identifier`	An identifier for this STIX Question. The **id** field for the Question is designed to help associate any related STIX Answer objects with the matching STIX Question.
spec_version (required)	`string`	The version of the STIX specification used to represent the content in this STIX Question. The value of this property **MUST** be `2.1` for STIX Questions containing STIX Objects defined in this specification.
created_by_ref (optional)	`identifier`	The **created_by_ref** property specifies the ID of the Identity object that describes the entity that created this STIX Question.

		If this attribute is omitted, the source of this information is undefined. This may be used by object creators who wish to remain anonymous.
expiry (optional)	`timestamp`	The **expiry** property represents the time at which the requester would like STIX Answers by. This field is purely informational for recipients of the STIX Question so that they know how long they have to produce a STIX Answer. Recipients MAY still create STIX Answers after the timeout period has expired, and the requester MAY accept STIX Answers after the expiry date/time has passed. The **expiry** timestamp **MUST** be precise to the nearest millisecond. It does not have a corresponding precision property and its precision **MUST** be treated as `full`.
questions (optional)	`list` of type `string`	An optional list of human readable questions that the requester would like someone in the community to answer. Questions SHOULD be added to the **questions** field only if they cannot be asked through use of the **objects**, **object_ids** or **observables** fields. **objects**, **object_ids** and **observables** fields should be preferred over the text based **questions** field as the structure of those fields better enables automation.
objects (optional)	`list` of type *`<STIX Object>`*	Specifies a set of one or more STIX Objects that the requester would like related intelligence about. Objects in this list **MUST** be a valid STIX Object (SDO, SRO or Custom Object). This allows the requester to include some STIX Objects in the STIX Question itself, just in case other members of the threat intelligence community don't have them.

object_ids (optional)	`list` of type `identifier`	Specifies a set of one or more STIX identifiers that the requester would like related intelligence about. Object identifiers in this list **MUST** be those from valid STIX Objects (SDO, SRO or Custom Objects).
observables (optional)	`list` of type *`<STIX Cyber Observable Object>`*	Specifies a set of one or more STIX Cyber Observable Objects that the requester would like related intelligence about. Objects in this list **MUST** be a valid STIX Cyber Observable Object (SDO, SRO or Custom Object).

5.2. Relationships

STIX Question is not a STIX Object and **MUST NOT** have any SRO-based relationships to it or from it. It **MAY** have a relationship to one or more STIX Answers.

5.3. Examples

```
{
  "type": "question",
  "id": "question--3b3f5235-41d3-4761-b6f8-fcf3c2fffed3",
  "spec_version": "2.1",
  "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
  "expiry": "2017-02-01T00:00:00Z",
  "questions": [
    "I need any information about the recent Mirai botnet updates. Which ISP are they targeting now?",
    "Does anyone know a good Incident Response company in New York they can recommend?",
    }
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-29T14:09:00.123456Z",
      "modified": "2016-04-29T14:09:00.123456Z",
      "object_marking_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],
      "name": "Poison Ivy Malware",
      "description": "This file is part of Poison Ivy",
      "pattern": "file-object.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3'"
    }
  ],
  "object_ids": [
    {
      "indicator--b01efc25-77b4-4003-b18b-f6e24b5cd9f7",
      "campaign--1626a5a5-2cc6-4724-81a7-7a9db549c61e",
      "threat-actor--45fbe659-dea3-43e9-9df4-b28d10fa37b7"
    }
  ],
  "observables": [
    {
      "type": "ipv4-addr",
      "value": "198.51.100.3"
```

```
    },
    {
      "type": "file",
      "hashes": {
        "MD5": "4472ea40dc71e5bb701574ea215a81a1"
      },
      "size": 25536,
      "name": "foo.dll"
      }
    }
  ]
}
```

STIX Answer

Type Name: `answer`	**Status:** Proposal **STIX 2.1**: Undecided

The STIX Answer message type is used to allow a member of a threat intelligence community to respond (the responder) to a request information from another member of the group (the requester). A STIX Answer MUST be related to a STIX Question object via the **question_ref** field.

Creating a STIX Answer to respond to a STIX Question is optional.

The responder MAY include any STIX Objects in the STIX Answer that it determines helps answer the question

STIX Answers MAY contain any STIX Objects that the responder believes will help provide useful information to the requester.

The STIX Answer is not a STIX Data Object or a STIX Relationship Object, so it does not have any of the Common Properties other than the **type**, **id** and **created_by_ref** fields. The STIX Answer is transient in nature, and implementations should not assume that other implementations will treat it as a persistent object.

The JSON MTI serialization uses the JSON object type <TODO: add reference> when representing `answer`.

. Properties

Property Name	Type	Description
type (required)	`string`	The value of this field **MUST** be `question`
id (required)	`identifier`	An identifier for this STIX Question. The **id** field for the Question is designed to help associate any related STIX Answer objects with the matching STIX Question.
spec_version (required)	`string`	The version of the STIX specification used to represent the content in this STIX Question. The value of this property **MUST** be `2.1` for STIX Questions containing STIX Objects defined in this specification.
question_ref (required)	`identifier`	The identifier of the STIX Question that this STIX Answer is attempting to answer. The **question_ref** field for is designed match STIX Answer object with the matching STIX

		Question.
created_by_ref (optional)	`identifier`	The **created_by_ref** property specifies the ID of the Identity object that describes the entity that created this STIX Question. If this attribute is omitted, the source of this information is undefined. This may be used by object creators who wish to remain anonymous.
answers (optional)	`list` of type `string`	A list of text answers to the text questions posed in the STIX Question object that this STIX Answer is responding to. Each text answer SHOULD correspond to a match question that was asked in the corresponding STIX Question. Text answers MAY be in any order, but SHOULD be in the same order that the text questions were asked in the corresponding STIX Question.
objects (optional)	`list` of type *`<STIX Object>`*	Specifies a set of one or more STIX Objects that the requester would like related intelligence about. Objects in this list **MUST** be a valid STIX Object (SDO, SRO or Custom Object). This allows the requester to include some STIX Objects in the STIX Question itself, just in case other members of the threat intelligence community don't have them.

5.2. Relationships

STIX Question is not a STIX Object and **MUST NOT** have any SRO-based relationships to it or from it. It **MUST** have a relationship to the STIX Question that it is trying to answer.

5.3. Examples

```
{
  "type": "answer",
  "id": "answer--3b3f5235-41d3-4761-b6f8-fcf3c2fffed3",
  "spec_version": "2.1",
  "created_by_ref": "identity--d8f5c954-4aba-43f3-b36b-c64f9c610953",
  "question_ref": "question--3b3f5235-41d3-4761-b6f8-fcf3c2fffed3",
  "answers": [
    "Mirai has been attempting to rollout firmware updates over the Antarctic ISP FrozenNet. Looks like a massive expansion into the polar bear market.",
```

```
    "Nope. I don't know of any New York IR companies sorry."
  ],
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",
      "created": "2016-04-29T14:09:00.123456Z",
      "modified": "2016-04-29T14:09:00.123456Z",
      "object_marking_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],
      "name": "Poison Ivy Malware",
      "description": "This file is part of Poison Ivy",
      "pattern": "file-object.hashes.md5 = '3773a88f65a5e780c8dff9cdc3a056f3'"
    }
  ]
}
```