# Interoperability Demonstration Guidelines for SDO Sponsors:

*Below are simple guidelines for completing the documentation of your sponsored SDO for the STIX 2.1 Sponsorships. These are due April 2nd, and should be performed quickly. I will put a placeholder for each Sponsor and each Use Case in Chapter 4 of each document.*

*March 14, 2019*

## Please Consider:

1. Define the high-level goals of sharing intelligence from both a producer and consumer's perspective.
    a. It is a good idea to define the tests based on the assumption that the producer and consumer are represented by 2 different organizations where they do not have access to a common data-store and therefore it mandates the use of TAXII to exchange their intelligence.
2. What are the requirements for producing content correctly?
    a. Describe in as much detail as possible what is the intended outcome once the produced intelligence is published what a consumer may use that intelligence for. This ensures that the intelligence is well-defined and fully qualified so that a consumer can act on the intelligence.
    b. Publishing incomplete or immature intelligence will result in consumers not knowing how to handle the missing data or worse causing them to act in a manner that is not intended by the producer of the intelligence.
3. What are the requirements for consuming it correctly?
    a. Describe in as much detail as possible what consuming intelligence means and how should a consumer respond. In most cases, consumers are also producers of similar intelligence or intelligence that is related to the received content. Describe as much as possible the interactions and relationships expected between different intelligence so that consumers can use shared intelligence from multiple providers effectively.
4. If bi-directional communications are required, what is the state exchange between the two personas as they exchange STIX SDOs?
    a. Typically, most effective sharing of intelligence is an exchange in both directions of related context. Either additional intelligence or additional context that may be attributed to the original intelligence such that a greater understanding is collectively achieved. That means, that individual objects are not often shared solely in isolation of other things. Describe in as much detail as possible what are the most common expected related context so that the testing includes those more comprehensive testing scenarios.
5. If its more than a 1-1 exchange but 1-n or n-n then what are the interactions that are expected?
    a. Describe in as much detail as possible the lifecycle of intelligence not just a single exchange of production and consumption. In most cases intelligence sharing environments will iterate on that intelligence over time with multiple perspectives contributing to the intelligence. What properties and relationships will occur and test those being set and updated.

**An Example:**

Assertion: the opinion object is intended to be a feedback mechanism on shared intel, therefore,

Step 0: Define what persona producers & consumers are likely to match the test flow. This will influence how the tests are performed and also the expected behaviors on production and consumption side.

i.e. a TIP; a DFP; a TMS (firewall)…etc

Step 1: What intel a producer has shared (start with a simple indicator)

Step 2: Publish that intel to a taxii server

Step 3: Assume *n* consumers pull that intel down

Step 4: Analyst reviews the indicator and determines either by looking at it or deploying and realizing its wrong wants to provide feedback to that indicator

Step 5: Analyst creates opinion with what the sponsor's consider relevant details

Step 6: Publish back to where?

Many data providers will not be setup for bi-directional communications. So, the group needs to decide how that will take place. Is it to the same collection with read-write permissions? It is a different collection with write-only collections?

Step 7: Somehow the original producer has to be checking for feedback.

This is where the provider reads the opinion back from a collection (read-write or write-only) and then cross correlates that opinion back to the original intel

Step 8: Original provider determines either change to original intel or do nothing.

If change then the cycle repeats but introduces new challenges because now the consumers must be able to determine that a new version of the original intel has been published and they should comment on that new version not the original