Diamond Model + STIX™ 2.1 = the CTI Diamond Sphere

Author: Nino Vincenzo Verde
March 14, 2020

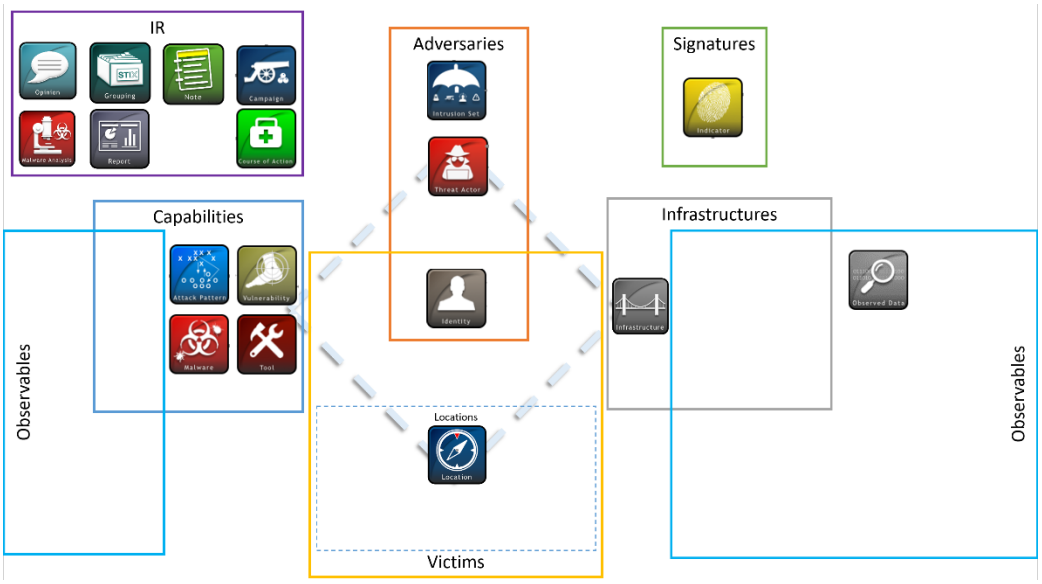
Despite the fact that STIX™ is the industry standards for Cyber Threat Intelligence (CTI), as a CTI analyst, I had always a lot of problems dealing with it. This is the reason I decided to share my taught in this document.

The first version of the standard was quite complicated and really heavy. With the introduction of STIX 2.0, I noticed that it was more close to the real needs of a CTI analyst. The latest draft (STIX 2.1 draft3), is even more promising in my opinion. So my question is: Is it the time to adopt it more heavily???

Most of the times, we base our day by day work on technologies or tools that support the STIX format as input or output. Sometimes, we use it at the end of an incident or analysis, that is when we have the need, and the will, to share the outcome with a community. But, how many of us are using the STIX data format to organize their CTI information?

In the CTI context, two models to take always into consideration are the killchain and the diamond model of intrusion analysis. Have you ever heard about the "28 buckets"??? If not… it's a pity… you should follow the SANS FOR578 course on Cyber Threat Intelligence. The basic idea, however, is quite simple: organizing your data into the seven phases of the killchain and the four vertices of the diamond model you will get 28 buckets or bins. The killchain is a property of five STIX™ Domain Objects, as for the latest draft that can be found here: https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.htm: `Attack Patterns`, `Indicators`, `Infrastructures`, `Malwares`, `Tools`. Therefore, it seems to be already addressed in STIX. But, what about the diamond model? A simple CTRL+F search on the same documentation cited above will give you a simple result: "Not Found"!!! Wait a moment… I use the diamond model every day, in 100% of my analysis, in 100% of my presentations… I know it is very useful in order to objectively evaluate CTI reports, and to make order in complex analysis. It is almost mandatory to use it when you want to understand your information gaps in order to fill out your RFI (requests for information). However… there is no trace of diamond model in STIX. For the sake of clarity, in the following I will use `this formatting` to highlight entities belonging to the STIX model (SDOs or SCOs, that are respectively STIX™ Domain Objects and STIX™ Cyber-observable Objects), and `this formatting` to highlight the four vertices of the diamond model.

In order to address the lack of any reference to the diamond model in STIX, I performed a very simple exercise: place each STIX SDOs/SCOs on a vertex of the diamond model. I had the hope to find a clear mapping among these two domains. Therefore, I started to fill `Adversaries`, `Victims`, `Infrastructures` and `Capabilities` vertices, and eventually, I came out with the following drawing:



Already at this point I had several considerations in mind, that I will report in the following:

1. There are SDOs that can go under more than one vertex of the diamond model. I rapidly figured out that the discriminant could be the type of relationship that these entities can have with other SDOs or SCOs. For example, let us consider the `Identity` SDO:
    a. if some entity, for example a `tool` or a `campaign`, has a relationship of type “targets” with an `identity`, then the `identity` becomes a `victim`. Indeed, “targets” is one of the permissible “reverse relationships” of an `identity` object. Simple and very straightforward.
    b. Then I thought: If an `identity` has a “targets” relationship with another `identity`, then it becomes an `Adversary`… but… wait a moment: `identities` can’t have relationships with other `identities` in the current version of the standard!!! My understanding is that you are obliged to use `Threat Actors` in these cases, and the further consideration is that a `threat-actor` can be “attributed-to” an `identity`. So: an `identity` that has a reverse relationship of type “attributed-to” can be considered an `Adversary`; furthermore, the same applies to the “impersonates” relationship.
2. `Capabilities` and `Infrastructures` are probably better described by the SCOs, that are for example: `Autonomous Systems`, `Domain Names`, `Email Addresses`, `IPv4 address`, etc. `Observed Data` seems to be the most appropriate entity to link SDOs with SCOs: indeed, it “conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs)”. So, my conclusion is that the `Observed Data` entity can be used as a special entity to describe both `Capabilities` and `Infrastructures`. However, the only relationships explicitly allowed by an `Observed Data` are reverse relationships from `Indicators` (rel. type “based-on”) or `Infrastructures` (rel. type “consists-of”). You shouldn’t use relationships, but the field called “object_marking_refs” to create links between `observed data` and SCOs. I think that this is counter intuitive and I would prefer to use explicit relationships. Probably I would leverage the common relationship “related-to”.
3. There are several SDOs that cannot be easily placed under any vertex of the diamond model. Therefore, I created two categories called Incident Response (IR) and Signatures to group them. Under the IR categories there are: `Opinion`, `Grouping`, `Note`, `Campaign`, `Malware Analysis`, `Report`, `Course of Action`. Under the Signature category there is only the `Indicator` SDO.

Lately, I figured out that the “pattern” field allows you to specify also appropriate languages, such as SNORT, Yara, Sigma, etc., thanks to OpenCTI.

4. Incident… where is the Incident SDO? Give me back the Incident SDOs!!! ☺
5. `Locations`: Often a `Threat Actor`, or an `Intrusion Set`, targets a particular Country or Region. This is well known to STIX 2.1 through the “targets” reverse relationship of `Location`, that is allowed with the following SDOs: `attack-pattern`, `campaign`, `intrusion-set`, `malware`, `threat-actor`, `tool`. The properties “region”, “country”, “latitude” and “longitude”, “city” must be leveraged for this purpose. These properties are hierarchically connected, and we should pay attention to univocally populate the parent field when we create new locations. Only in this way, in the future, we will be able to query, for example, all the `threat-actors` that targeted a Region without missing any record.
6. Real world events are often useful to link nefarious activities. Let us think to the Olympics Games, or the Presidential Elections. I didn’t find a correct way to express them in STIX yet, at least as SDOs.
7. I think that the `User-Account` SCO can be related to an `identity` or to a `threat actor`, but I didn’t find the correct way to represent a relationship between these objects, yet.

With all these considerations, I updated my PowerPoint and I come out with the following drawing. Now, if you have a foldable monitor, please put it in full screen mode and try to wrap it around a ball: you achieved the CTI Diamond Sphere.