STIX & The Cyber Asset Concept
Why you should use the (abstracted) Asset concept in CTI

2015-12-14 Jerome Athias

In CTI you want to know (collect/aggregate/correlate) and share Who, What, When, Where, How, Why.

Assuming that at some abstracted level:
A Cyber Asset (that could be an "Agent", or "Actor", or "Party", or "Group of") is always:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a lock, a device, etc.)

Who

Some concepts/objects/constructs in the current CTI Information Model *cover* the Who:

Threat_Actor ("malicious actors or adversaries")
Ref. https://stixproject.github.io/data-model/1.2/ta/ThreatActorType/
Expressed as an **Identity**
Ref. https://stixproject.github.io/data-model/1.2/stixCommon/IdentityType/
Expressed, by default, as CIQIdentity3
Why are we using the version 3.0 of the OASIS CIQ-PIL schema for structured characterization of Identities?
Because I asked for it some years ago. Why? To be compatible with the Asset Identification specification (NISTIR7693) http://scap.nist.gov/specifications/ai/

Question: could a Threat_Actor always be characterized (or abstracted) as one (or a group of)?:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

What

AffectedAsset
https://stixproject.github.io/data-model/1.2/incident/AffectedAssetType/

Could the enumeration here https://stixproject.github.io/data-model/1.2/stixVocabs/AssetTypeVocab-1.0/
be abstracted to:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

?

Exploit_Target "vulnerabilities or weaknesses in software, systems, networks or configurations that are targeted for exploitation by the TTP of a ThreatActor"
https://stixproject.github.io/data-model/1.2/et/ExploitTargetType/

Question: is an Exploit_Target always related to:

- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)

Question: if Exploit_Target was abstracted to a concept of Target, or Victim; could it be characterized (or abstracted) as one (or a group of)?:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

In this case, Question: could an Exploit_Target could be both What and Who?

Incident
https://stixproject.github.io/data-model/1.2/incident/IncidentType/
"Incidents are discrete instances of Indicators affecting an organization along with information discovered or decided during an incident response investigation. They consist of data such as time-related information, parties involved, **assets** affected, impact assessment, related Indicators, related Observables, leveraged TTP, attributed Threat Actors, intended effects, nature of compromise, response Course of Action requested, response Course of Action taken, confidence in characterization, handling guidance, source of the Incident information, log of actions taken, etc."

Question: is an Incident always involving one or more (group(s) of)?:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

Course of Action (COA)
https://stixproject.github.io/data-model/1.2/coa/CourseOfActionType/

Question: is an COA always involving one or more (group(s) of)?:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person

- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

Questions

From a storage point of view…
Is there a real need to store multiple times (duplicates) basics information (*identification*) regarding one Organization or a Person?

(NB: yes information can change and evolve other time, but GUIDs should be Global and Universal)

Could an Organization, or a Person, or an IT-Asset (e.g. a website) be one Threat_Actor for an Organization one day, and an Exploit_Target/Victim for another Organization the same day at the same time?

Could an Organization, or a Person, or an IT-Asset (e.g. a website) be "good/trusted" for an Organization one day and considered a Threat_Actor another day?

Could the Trust concept be applied (and change other time) on:

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

To something else?

Could a Threat_Actor's AssociatedActor be also a Threat_Actor (a Responder, a Victim…)?

Issues in the current CTI Information/Data Model

Not intended to be exhaustive, and main scope limited to the Asset concept.

InformationSource vs Identity

Example Incident:
https://stixproject.github.io/data-model/1.2/incident/IncidentType/

Reporter0..1	InformationSourceType	The Reporter field details information about the reporting source of this Incident.
Responder0..n	InformationSourceType	The Responder field is optional and details information about the assigned responder for this Incident.
Coordinator0..n	InformationSourceType	The Coordinator field is optional and details information about the assigned coordinator for this Incident.
Victim0..n	IdentityType	The Victim field is optional and details information about a victim of this Incident.

Should a Victim “limited to” a Person?
Could a Victim and a Reporter be one of (or a Group of):

- An Organization (e.g.: a country, an enterprise, a company, etc.)
- A Person
- An Automaton (or an IT-Asset, e.g.: system, network, database, software, website…)
- A Physical object (e.g.: a building, a door, a lock, a device, etc.)

Something else?

From a storage point of view (and also from a number of bits other the wire point of view):
Could a Reporter be also at some point a Responder, a Coordinator, a Victim, a Threat_Actor…?

Tool

https://stixproject.github.io/data-model/1.2/cyboxCommon/ToolInformationType/
If a Tool is always a Software (*one of Asset*), could/should it be identified using CPE?

Vendor0..1 string This field contains information identifying the vendor organization for this tool.

From a storage point of view (and also from a number of bits other the wire point of view):
Should the Vendor Organization a string here and a construct elsewhere?

Could a Tool be also an AffectedSoftware?
https://stixproject.github.io/data-model/1.2/et/AffectedSoftwareType/

COA vs Activity

https://stixproject.github.io/data-model/1.2/stixCommon/ActivityType/