STIX 2.0 Specification - Pre-Draft

TLO - TTPs - Version 0.2

Document Table of Contents

- 1. TTP Top Level Objects
  - 1.1. Attack Pattern
    - 1.1.1. Properties
    - 1.1.2. Relationships
  - 1.2. Exploit
    - 1.2.1. Properties
    - 1.2.2. Relationships
  - 1.3. Kill Chain
    - 1.3.1. Properties
    - 1.3.2. Relationships
  - 1.4. Kill Chain Phase
    - 1.4.1. Properties
    - 1.4.2. Relationships
  - 1.5. Malicious Infrastructure
    - 1.5.1. Properties
    - 1.5.2. Relationships
  - 1.6. Malicious Tool
    - 1.6.1. Properties
    - 1.6.2. Relationships
  - 1.7. Malware
    - 1.7.1. Properties
    - 1.7.2. Relationships
  - 1.8. Persona
    - 1.8.1. Properties
    - 1.8.2. 2.8.2.Relationships
  - 1.9. Victim Targeting
    - 1.9.1. Properties
    - 1.9.2. Relationships

Document Development Status

TODO - This section should be removed from the document prior to completion. It is included here to help visually track where things are at in the process.

Each physical documents contains a table that defines 4 levels of development for each TLO and CTI concept. The first level is called Concept. Content coming in to one of the documents starts as a Concept. Once the community starts to work on it it will move to Development. During this phase, the group will flesh out the design and come up with normative text. As the group comes to general consensus the TLO will move to a Review phase. During this phase the community can comment and offer suggestions on the normative text and design. After a period of time of no comments or feedback, the TLO will move to its final stage of Draft.

Object / Concept	Status	MVP
`attack-pattern`	Concept	Yes
`exploit`	Concept	Undecided
`kill-chain`	Concept	Undecided
`kill-chain-phase`	Concept	Undecided
`malicious-infrastructure`	Concept	Undecided
`malicious-tool`	Concept	Undecided
`malware`	Concept	Undecided
`persona`	Concept	Undecided

1. TTP Top Level Objects

In cyber threat intelligence, TTPs represent the tactics, techniques, and procedures that are used to carry out attacks. TTPs are a type of top-level object: the attack pattern, exploit, infrastructure, malware, persona, tool, and victim targeting top-level objects are all types of TTPs.

1.1. Attack Pattern

Type Name: `attack-pattern`	**Status:** Concept **MVP**: Yes

Attack Pattern describes a general approach for attacking a system or network. In addition to the standard TTP properties, it has a reference to a CAPEC (Common Attack Pattern Enumeration and Classification - http://capec.mitre.org/) ID.

Open Questions:

1. Jason K. had a proposal for all these external IDs to use our standard external IDs structure. That was back when external IDs were actually on the object though, now that you have to use a relationship it would be 2 additional TLOs just to say the CAPEC ID.

1.1.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `attack-pattern`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`capec_id` (optional)	`string`	Specifies a reference to an entry in the CAPEC dictionary.
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.1.2. Relationships

These are the default relationships between the Attack Pattern Object and other objects.

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Attack Pattern to the phase of the Kill Chain it is used within.

1.2. Exploit

Type Name: `exploit`	**Status:** Concept **MVP**: Undecided

Exploit describes a cyber threat exploit: a set of commands that leverages a vulnerability or misconfiguration (exploit target) in order to cause unintended behavior in the targeted software.

Open Question:

- This is a stub in STIX 1.x...can we just call it not MVP?

1.2.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `exploit`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.2.2. Relationships

These are the default relationships between the Exploit Object and other objects.

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Exploit to the phase of the Kill Chain it is used within.

1.3. Kill Chain

Type Name: `kill-chain`	**Status:** Concept **MVP**: Undecided

Kill chain describes the typical steps that attackers use to carry out their objectives. One popular example of a kill chain is the Lockheed Martin kill chain. Each phase of the Kill Chain is described in a separate object called a Kill Chain Phase. The distinction was made between Kill Chains and Kill Chain Phases to enable exploits to refer directly to individual phases of a kill chain.

Open Questions:

1. How do we support representing the ordinality of a kill chain phase within a kill chain?
2. Do kill chains even need to be TLOs? Can't we more easily solve this with controlled vocabularies?

1.3.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**

type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `kill-chain`
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.3.2. Relationships

These are the default relationships between the Kill Chain Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`has-kill-chain-phase`	`kill-chain-phase`	Relates the Kill Chain to the Kill Chain Phase.

1.4. Kill Chain Phase

Type Name: `kill-chain-phase`	**Status:** Concept **MVP**: Undecided

Kill chain phase describes an individual phase of a Kill Chain that attackers use to carry out their objectives. One popular example of a kill chain is the Lockheed Martin kill chain. This Kill Chain Phase describes one phase of a Kill Chain. The distinction was made between Kill Chains and Kill Chain Phases to enable exploits to refer directly to individual phases of a kill chain.

1.4.1. Properties

STIX TLO Common Properties

type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings		
Property Name	**Type**	**Description**
type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `kill-chain-phase`
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.4.2. Relationships

These are the default relationships between the Kill Chain Phase Object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain`	`kill-chain`	Relates the Kill Chain Phase to the phase of the Kill Chain it belongs to. Requires an extension with the name `ordinality` to indicate the ordinality of the phase within the Kill Chain.

1.5. Malicious Infrastructure

Type Name: `malicious-infrastructure`	**Status:** Concept **MVP**: Undecided

Infrastructure describes infrastructure leveraged by cyber threat actors, such as command and control servers, domain registration, botnets, or hosting/delivery.

Open Question:

- How do you characterize the technical information (IPs, etc.) for the infrastructure?

1.5.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `malicious-infrastructure`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`labels` (required)	`array` of type `malicious-infrastructure-label-cv`	The kind(s) of infrastructure being described.
`labels_ext` (optional)	`array` of type `vocab-ext`	Specifies alternate values for the **`labels`** property.
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.5.2. Relationships

These are the default relationships between the Malicious Infrastructure Object and other objects.

Inherited From	**Inherited Kinds of Relationships**
`stix-core`	`duplicate-of`, `other`

Kind of Relationship	Target	Description
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Malicious Infrastructure to the phase of the Kill Chain it is used within.

1.6. Malicious Tool

Type Name: `malicious-tool`	**Status:** Concept **MVP**: Undecided

Tool describes a piece of software designed with a malicious purpose that is used directly by an attacker.

Open Questions:

- Is the subtle difference between this TLO and malware necessary to represent?
- Should we merge the Malware TLO with this TLO and just have a boolean value that is **`is_malware`** ?

1.6.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `malicious-tool`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`labels` (required)	`array` of type `malicious-tool-`	The kind(s) of tool(s) being described.

	`label-cv`	
`labels_ext` (optional)	`array` of type `vocab-ext`	Specifies alternate values for the **`labels`** property.
`compensation_model` (optional)	`string`	The type of compensation model used by this tool.
`tool_information_ref` (required)	`identifier`	The characterization of the tool itself. This **MUST** refer to a Tool TLO.
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.6.2. Relationships

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Malicious Tool to the phase of the Kill Chain it is used within.

1.7. Malware

Type Name: `malware`	**Status:** Concept **MVP**: Undecided

Malware describes software designed specifically with a malicious purpose by a malicious threat actor often installed without the user of the system being aware. This DOES NOT include software created for legitimate purposes which are then abused by threat actors for their own purposes.

Open Questions:

- Should malware be merged into malicious tool?

1.7.1. Properties

STIX TLO Common Properties		
type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings		
Property Name	**Type**	**Description**
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
labels (required)	`array` of type `malware-label-cv`	The kind(s) of malware being described.
labels_ext (optional)	`array` of type `vocab-ext`	Specifies alternate values for the **labels** property.
maec (optional)	*MAEC*	A description of the malware leveraging MAEC.
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.7.2. Relationships

These are the default relationships between a Malware Object and other objects.

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Malware to the phase of the Kill Chain it is used within.

1.8. Persona

Type Name: `persona`	**Status:** Concept **MVP**: Undecided

Persona captures a false identity leveraged by a threat to masquerade as another party.

Open Questions:

1. Is this a separate TLO, or is it a relationship (uses-persona) from a threat actor to an identity?
2. Regardless of how persona is defined, it needs to be a many-to-many relationship between threat actors and personas.

1.8.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `persona`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.8.2. 2.8.2.Relationships

These are the default relationships between a Persona and other objects.

Inherited From	**Inherited Kinds of Relationships**
`stix-core`	`duplicate-of`, `other`

Kind of Relationship	Target	Description
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Persona to the phase of the Kill Chain it is used within.

1.9. Victim Targeting

Type Name: `victim-targeting`	**Status:** Concept **MVP**: Undecided

Victim targeting describes the types of victims targeted by a particular threat. This includes identity-based targeting (by sector, company, country, etc.), system-based targeting (web systems, etc), or information type-based targeting (credentials, PII, trade secrets, etc.).

Open Questions:

- This is a stub, we need to define what all can be a target
- How much of this should be relationships to assets, identities, etc? Can you represent combinations of these (HR information in energy sector) via relationships?

1.9.1. Properties

STIX TLO Common Properties		
`type, id, created_by_ref, created_time, revision, modified_time, revoked, revision_comment, confidence, object_markings_refs, granular_markings`		
Property Name	**Type**	**Description**
`type` (required)	`string`	The value of this field MUST be `victim-targeting`
`title` (optional)	`string`	A human readable title
`description` (optional)	`string`	A human readable description
`targets` (required)	`array` of type `identity-target`, `system-target`,	The list of targets.

	`information-target`	
`severity` (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

1.9.2. Relationships

These are the default relationships between a Victim Targeting object and other objects.

Inherited From		**Inherited Kinds of Relationships**
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`in-kill-chain-phase`	`kill-chain-phase`	Relates the targeting to the phase of the Kill Chain it is used within.