STIX 2.0 Specification - Pre-Draft

TLO - Exploit Targets - Version 0.2

Document Table of Contents

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
`exploit-target` (abstract)	Concept	Undecided

`configuration`	Concept	Undecided
`vulnerability`	Concept	Undecided
`weakness`	Concept	Undecided

1. Top Level Objects

1.1. Exploit Target

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

Exploit targets represent the things about the defender's systems that make them vulnerable to attack by a threat actor. In STIX, Exploit Targets may be configurations, vulnerabilities, or weaknesses.

`exploit-target` can be considered an "abstract superclass" of the individual Exploit Target types listed below. Common properties that apply to all Exploit Targets are defined on `exploit-target` and inherited by the individual Exploit Target types.

As an abstract superclass, `exploit-target` *cannot be directly instantiated.*

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 `exploit-target`
`title` (optional)	`string`	A human readable title

description (optional)	`string`	A human readable description
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

2. Exploit Target Objects

2.1. Configuration

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

Leverages CCE (https://nvd.nist.gov/cce/index.cfm) to describe a configuration setting that may present a target for an attacker.

2.1.1. 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 `configuration`
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
cce_id (optional)	`string`	The CCE ID for this configuration.
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

2.1.2. Relationships

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

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target Type**	**Description**
`evidenced-by`	`observation`	Relates the Configuration to an Observation providing evidence that backs up the assertions provided in this Object.
`exploited-by`	`exploit`	Relates the Configuration to an Exploit that can take advantage of a misconfiguration.
`in-kill-chain-phase`	`kill-chain- phase`	Relates the Configuration to the phase of the Kill Chain it is used within.

2.2. Vulnerability

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

Leverages CVE (http://cve.mitre.org/) to describe a particular vulnerability that may present a target for an attacker.

2.2.1. 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`	The value of this field MUST be `vulnerability`
`title` (optional)	`string`	A human readable title

description (optional)	`string`	A human readable description
cve_id (optional)	`string`	The CVE ID for this vulnerability.
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

2.2.2. Relationships

TODO

2.3. Weakness

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

Leverages CWE (http://cwe.mitre.org/) to describe a software weakness that may present a target for an attacker.

2.3.1. 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**
title (optional)	`string`	A human readable title
description (optional)	`string`	A human readable description
cwe_id (optional)	`string`	The CWE ID for this weakness.
severity (reserved)	`RESERVED`	RESERVED FOR FUTURE USE

2.3.2. Relationships

These are the official relationships to describe a relationship between the Weakness Object and other objects.

Inherited From		Inherited Kinds of Relationships
`stix-core`		`duplicate-of`, `other`
Kind of Relationship	**Target**	**Description**
`evidenced-by`	`observation`	Relates the Weakness to an Observation providing evidence that backs up the assertions provided in this Object.
`exploited-by`	`exploit`	Relates the Weakness to an exploit that can exploit the vulnerability.
`in-kill-chain-phase`	`kill-chain-phase`	Relates the Weakness to the phase of the Kill Chain it is used within.