STIX 2.0 Specification - Pre-Draft

TLO - Exploit Targets - Version 0.1

Document Table of Contents

1. Document Development Status

Object / Concept	Status	MVP	Description
`exploit-target` (abstract)	Concept	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. *As an abstract superclass,* `exploit-target` *cannot be directly instantiated.*
`configuration`	Concept	Undecided	Leverages CCE to describe a system configuration that may be exploited as part of an attack.

`vulnerability`	Concept	Undecided	A flaw in software that may be exploited as part of an attack. Uses CVE.
`weakness`	Concept	Undecided	A category of weakness that may be exploited as part of an attack. Uses CWE.

2. Top Level Objects

2.1. 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.*

2.1.1. Properties

Inherits From	Inherited Properties	
`stix-core`	**`type`, `id`, `spec_version`, `created_time`, `created_by_ref`, `object_markings_refs`, `granular_markings`**	
`descriptive-properties`	**`title`, `description`**	
Property Name	**Type**	**Description**

type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `exploit-target`
impact (optional)	`impact`	The impact on operations if this exploit target were to be realized.

3. Exploit Target Objects

3.1. 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.

3.1.1. Properties

Inherits From	Inherited Properties	
`stix-core`	**type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings**	
`descriptive-properties`	**title, description**	
`exploit-target`	**impact**	
Property Name	**Type**	**Description**
type (required)	`string`	(Overrides `stix-core`) The value of this field **MUST** be `configuration`
cce_id (optional)	`string`	The CCE ID for this configuration.

3.1.2. Relationships

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

Inherited From		Inherited Kinds of Relationships
`stix-core`		`derived-from`, `duplicate-of`, `suggested-update`, `related-to`
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.

3.2. 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.

3.2.1. Properties

Inherits From	Inherited Properties
`stix-core`	**`type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings`**

`descriptive-properties`	**`title, description`**
`exploit-target`	**`impact`**

Property Name	Type	Description
`type` (required)	`string`	The value of this field MUST be `vulnerability`
`cve_id` (optional)	`string`	The CVE ID for this vulnerability.

3.2.2. Relationships

TODO

3.3. 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.

3.3.1. Properties

Inherits From	Inherited Properties
`stix-core`	**`type, id, spec_version, created_time, created_by_ref, object_markings_refs, granular_markings`**
`descriptive-properties`	**`title, description`**
`exploit-target`	**`impact`**

Property Name	Type	Description
`cwe_id` (optional)	`string`	The CWE ID for this weakness.

3.3.2. 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`		`derived-from`, `duplicate-of`, `suggested-update`, `related-to`
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.