STIX2 Cheat Sheet

by apowers313 via cheatography.com/31528/cs/21286/

About

Structured Threat Information Expression (STIX™) is JSON schema and vocabulary for communicating cyber threat intelligence (CTI), such as attacks, malware, threat actors, and mitigations. The STIX specification is managed by OASIS.

Example Attack Pattern

```
{
      "type": "attack-pattern",
      "id": "attack-pattern--18-
3dcab1-9bd1-4973-aede-0e2ab018-
3d11",
      "name": "Example Attack",
      "description": "An example
'technique' or attack.",
      "x_mitre_detection": "A
short description of how the
attack can be detected.",
      "created_by_ref": "identi-
ty--b9e8b9fd-6d27-472b-bfee-3f-
6501edf3e9",
      "created": "2017-12-14T1-
6:46:06.044Z",
      "modified": "2019-06-13T1-
4:49:56.024Z",
      "kill_chain_phases": [
        {
          "kill_chain_name": "-
example-kill-chain",
          "phase_name": "initia-
l-access"
        }
      ],
      "x_mitre_version": "1.0",
      "external_references": [
        {
          "external_id": "ID1-
23",
          "source_name": "exa-
mple-attack",
```

Example Attack Pattern (cont)

```
          "url": "https://exam-
ple.org/attack/ID123"
        }
      ]
    }
```

Object Types

Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
Course of Action	An action taken to either prevent an attack or respond to an attack.
Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.

Object Types (cont)

Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
Observed Data	Conveys information observed on a system or network (e.g., an IP address).
Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
Tool	Legitimate software that can be used by threat actors to perform attacks.

By **apowers313**

cheatography.com/apowers313/
ato.ms

Not published yet.
Last updated 13th February, 2022.

Object Types (cont)	
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Relationship	Used to link two SDOs and to describe how they are related to each other.
Sighting	Denotes the belief that an element of CTI was seen (e.g., indicator, malware).

By **apowers313**

cheatography.com/apowers313/
ato.ms

Not published yet.
Last updated 13th February, 2022.