**STIX Enforcer**

The STIX Enforcer consists of a series of scripts which when run on a STIX bundle will make various corrections to the bundle for commonly made errors. These are referred to as “Fixers”. STIX Enforcer also can check for presence of other “required” (optional in the STIX specification) properties and elements. This can be considered a stricter STIX validator. These are referred to as “Checkers”. Additionally, STIX Enforcer can apply place holder values within a bundle for missing properties. These are referred to as “Holders”. Fixers and Holder modify the inputted STIX bundle, while Checkers only notify the user of missing “required” components. Each script is designed to be run independently if needed to check or fix a specific property, but are to be run together with the STIX Enforcer.py script

|  |  |
| --- | --- |
| Object Type | Enforced Properties (Previously Optional) |
| Vulnerability | description, external\_references[source\_name, external\_id, cve] |
| Software | cpe, version, vendor |
| Grouping | name, description |
| Indicator | name, description, kill\_chain\_phases |
| Location | name, description |
| Malware | name description, kill\_chain\_phases, malware\_types, Related File SDO |
| File | name, hashes |
| Attack Pattern | description, kill\_chain\_phases, external\_references[source\_name, external\_id, capec] |
| Tool | kill\_chain\_phases |
| Infrastructure | kill\_chain\_phases, description |
| Intrusion Set | description |
| Report | description |
| Threat Actor | description |
| Note | author |
| Opinion | author |
| Network Traffic | src\_port, dst\_port |
| Campaign | description |
| Identity | description |
| Course of Action | description |

|  |  |
| --- | --- |
| Element | Enforced Requirement |
| Description | Must be a minimum of 10 words in length |
| UUIDs | Must be of correct type (UUID4 vs UUID5) for each SDO |
| Time | Must be in the expected time format |
| Verbiage | Relationship titles must match the STIX specification |

**Usage**

* Download Requirements:
* pip install -r requirements.txt
* Run Enforcer
* python STIX\_Enforcer.py [Path to STIX JSON Input Bundle] [Path to STIX JSON Output Bundle] [(optional:) > Path to Printing Output]

**Note:** If only path to one bundle is provided as an argument, then it is considered both the input

and the output and file overwriting will occur

**Fixers (3 Total)**

|  |  |
| --- | --- |
| Fixer | Description |
| UUID5 | Replaces UUIDs from SCOs with UUID5s (Replacement made throughout file) |
| Timestamp | Ensures proper timestamp formatting |
| Verbiage | Ensures that the correct relationship type is used based on the source and target |

**Holders (11 Total)**

|  |  |
| --- | --- |
| Holder | Description |
| AttackPatternReqHolder | Applies place holder values for missing ‘external\_references’, ‘source\_name’, ‘capec’ and ‘external\_id’ properties in attack-pattern SDOs |
| AuthorReqHolder | Applies place holder values for missing ‘author’ property in various SDOs |
| DescLenHolder | Buffers ‘description’ on various SDOs to meet the minimum length of 10 words |
| DescReqHolder | Applies place holder values for missing ‘description’ property in various SDOs |
| FileReqHolder | Applies place holder values for missing ‘hashes’ property in file SDOs |
| KillChainReqHolder | Applies place holder values for missing ‘kill\_chain\_phases’ property in various SDOs |
| MalwareReqHolder | Applies place holder values for missing ‘malware\_types’ property in malware SDOs |
| NameReqHolder | Applies place holder values for missing ‘name’ property in various SDOs |
| NetworkTrafficReqHolder | Applies place holder values for missing ‘src\_port’ and ‘dst\_port’ property in network-traffic SDOs |
| SoftwareReqHolder | Applies place holder values for missing ‘cpe’, ‘version’, ‘vendor’ property in software SDOs |
| VulnerabilityReqHolder | Applies place holder values for missing ‘external\_references’, ‘source\_name’, ‘cve and ‘external\_id’ properties in vulnerability SDOs |

**Checkers (12 Total)**

|  |  |
| --- | --- |
| Checker | Description |
| AttackPatternReqChecker | Checks for presence of ‘external\_references’, ‘source\_name’, ‘capec’ and ‘external\_id’ properties in attack-pattern SDOs |
| AuthorReqChecker | Checks for presence of ‘author’ property in various SDOs |
| DescLenChecker | Checks for SDO descriptions that are less than 10 words in length |
| DescReqChecker | Checks for presence of ‘description’ property in various SDOs |
| FileReqChecker | Checks for presence of ‘hashes’ property in file SDOs |
| KillChainReqChecker | Checks for presence of ‘kill\_chain\_phases’ property in various SDOs |
| MalwareReqChecker | Checks for presence of ‘malware\_types’ property in malware SDOs |
| NameReqChecker | Checks for presence of ‘name’ property in various SDOs |
| NetworkTrafficReqChecker | Checks for presence of ‘src\_port’ and ‘dst\_port’ property in network-traffic SDOs |
| SoftwareReqChecker | Checks for presence of ‘cpe’, ‘version’, ‘vendor’ property in software SDOs |
| VulnerabilityReqChecker | Checks for presence of ‘external\_references’, ‘source\_name’, ‘cve and ‘external\_id’ properties in vulnerability SDOs |
| MalwareFileReqChecker | Checks for presence of associated file SDO and relationship objects from malware SDOs |

**Note for Developers:**

There is a standard to how new fields to enforce are to be implemented. Any fixer or checker will be put in the appropriate folder. This is because STIX\_Enforcer.py uses system calls to go through each folder and run each file. An example of the proper way to ensure a file will run given the system arguments is given below. On another note, output should follow the standard set in place. If an object is changed or flagged, please print the appropriate UUID.

Text

Description automatically generated