TLP Marking Definition Version 2.0 for STIX™ Version 2.1

Final

1 October 2022

​Editors:

TBD

Additional artifacts:

* TRAFFIC LIGHT PROTOCOL (TLP**):** FIRST Standards Definitions and Usage Guidance — Version 2.0

This prose specification is one component of a Work Product that also includes:

* STIX™ Version 2.1 – OASIS specification

Related work:

This specification replaces or supersedes:

* *N/A*

Abstract:

The Traffic Light Protocol (TLP) version 2.0 was developed by the Forum of Incident Response and Security Teams (FIRST).  TLP provides a simple and intuitive schema for indicating with whom potentially sensitive information can be shared. This document defines the approach to express TLP 2.0 using Structured Threat Information Expression (STIXTM) language via the use of a marking definition object.

# 1.​ Data Markings in STIX

Data markings represent restrictions, permissions, and other guidance for how data can be used and shared. For example, data may be shared with the restriction that it must not be re-shared, or that it must be encrypted at rest. In STIX, data markings are specified using the marking-definition object. For general information on data markings in STIX, see section 7.2 of STIX™ Version 2.1 - OASIS specification.

### 2. **The Traffic Light Protocol (TLP)** Marking Object Type

The Traffic Light Protocol (TLP) marking definition type, version 2.0, defines the STIX object types required to share the TLP 2.0 standard developed by Forum of Incident Response and Security Teams (FIRST). TLP was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information *source*, towards one or more *recipients*.  TLP data markings are defined using the “colors” of a traffic light.

Because TLP 2.0 data markings are not part of the STIX 2.1 specification, they must be specified using the Extension Definition object as described in section 7.3 of the specification.

The tables below describe the properties of a STIX 2.1 TLP 2.0 marking definition type. These properties are based on the marking-definition object type described in section 7.2 of the STIX 2.1 specification. Notice that the deprecated properties of the marking definition object type are not used.

|  |  |  |
| --- | --- | --- |
| **Required Common Properties** | | |
| **type**, **spec\_version**, **id**, **created**, **extensions** | | |
| **Optional Common Properties** | | |
| n/a | | |
| **Not Applicable Common Properties** | | |
| **confidence**, **defanged**, **created\_by\_ref**, **external\_references**, **granular\_markings**, **labels**, **lang**, **modified**, **object\_marking\_refs**, **revoked** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The **type** property identifies the type of object. The value of this property **MUST** be marking-definition. |
| **name** (required) | string | A name used to identify the Marking Definition.  The value of this property **MUST** be one of the following:  TLP:CLEAR  TLP:GREEN  TLP:AMBER  TLP:AMBER+STRICT  TLP:RED |
| **extensions** (required) | dictionary | Specifies the TLP 2.0 marking “color” as an extension dictionary.  There **MUST** be only one dictionary key and it **MUST** be **extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d**, which is the id of the extension-definition object associated with TLP-2.0.  The corresponding dictionary values **MUST** be the tlp-2-0-description data type described below. |

**Type Name:** tlp-2-0-description

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **extension\_type** (required) | string | The **extension\_type** property indicates the type of extension is being used. The value of this property **MUST** be property-extension |
| **tlp\_2\_0** (required) | string | This property contains TLP 2.0 “color”. It must be one of the following:  clear,  green,  amber,  amber+strict,  red |

The following standard marking definitions **MUST** be used to reference or represent TLP 2.0 markings. Other instances of a TLP 2.0 marking definition object **MUST NOT** be used or created (the only instances of TLP 2.0 marking definitions permitted are those defined here).

|  |  |
| --- | --- |
| clear | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--94868c89-83c2-464b-929b-a1a8aa3c8487",  "created": "2022-10-01T00:00:00.000Z",  "name": "TLP:CLEAR",  "extensions": {  "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {  "extension\_type": "property-extension",  "tlp\_2\_0": "clear"  }  }  } |
| green | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition---bab4a63c-aed9-4cf5-a766-dfca5abac2bb",  "created": "2022-10-01T00:00:00.000Z"  "name": "TLP:GREEN",  "extensions": {  "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {  "extension\_type": "property-extension",  "tlp\_2\_0": "green"  }  }  } |
| amber | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition---55d920b0-5e8b-4f79-9ee9-91f868d9b421",  "created": "2022-10-01T00:00:00.000Z"  "name": "TLP:AMBER",  "extensions": {  "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {  "extension\_type": "property-extension",  "tlp\_2\_0": "amber"  }  }  } |
| amber+strict | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition---939a9414-2ddd-4d32-a0cd-375ea402b003",  "created": "2022-10-01T00:00:00.000Z",  "name": "TLP:AMBER+STRICT",  "extensions": {  "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {  "extension\_type": "property-extension",  "tlp\_2\_0": "amber+stict"  }  }  } |
| red | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--e828b379-4e03-4974-9ac4-e53a884c97c1",  "created": "2022-10-01T00:00:00.000Z",  "name": "TLP:RED",  ""extensions": {  "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d": {  "extension\_type": "property-extension",  "tlp\_2\_0": "red"  }  }  } |

In general, there is no need to share a TLP 2.0 marking-definition object in a Bundle, because all STIX compliant implementations must be aware of these five objects. Use the id property of these objects to mark content.

# Extension Definition Object for TLP 2.0

{

"id": "extension-definition--60a3c5c5-0d10-413e-aab3-9e08dde9e88d",

"type": "extension-definition",

"spec\_version": "2.1",

"name": "TLP 2.0",

"description": "This defines TLP 2.1 as a STIX extension",

"created": "2022-10-01T00:00:00.000Z",

"modified": "2022-10-01T00:00:00.000Z",

"created\_by\_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",

"schema": "https://github.com/oasis-open/cti-stix-common-objects/tree/master/extension-definition-specifications/tlp-2.0",

"version": "1.0.0",

"extension\_types": [

"property-extension"

]

}