PAP Marking Definition for STIX™ Version 2.1

Draft

28 November 2022

​Editors:

Jill Kamienski

Additional artifacts:

* Permissible Actions Protocol (PAP) MISP Taxonomy

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 Permissible Actions Protocol (PAP) used in MISP is a protocol that describes how much risk of an attacker detecting current analysis state or defensive actions is acceptable. It is designed to indicate what the receiver may do with the information, and it achieves this by using a color scheme. PAP provides a focus on what defenders are **allowed** to do with information they receive. This document defines the approach to express PAP 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 Permissible Actions Protocol (PAP)** Marking Object Type

The Permissible Actions Protocol (PAP) marking definition type defines the STIX object types required to share the PAP standard used by MISP. PAP was created to facilitate greater sharing of potentially sensitive information and more effective collaboration, with a focus on what recipients are allowed to do with the information. Some actions taken by defenders could alert attackers to the fact that they are aware of the attack or where they are in their analysis. This such actions should be limited, and PAP provides a way of describing such limitations. PAP data markings are defined using the “colors” of a traffic light.

Because PAP 1.0 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 PAP 1.0 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:  PAP:WHITE  PAP:GREEN  PAP:AMBER  PAP:RED |
| **extensions** (required) | dictionary | Specifies the PAP marking “color” as an extension dictionary.  There **MUST** be only one dictionary key and it **MUST** be **extension-definition--** **f8d78575-edfd-406e-8e84-6162a8450f5b**, which is the id of the extension-definition object associated with PAP.  The corresponding dictionary values **MUST** be the pap-description data type described below. |

**Type Name:** pap-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 |
| **pap** (required) | string | This property contains PAP “color”. It must be one of the following:  white,  green,  amber,  red |

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

|  |  |
| --- | --- |
| white | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition-- a3bea94c-b469-41dc-9cfe-d6e7daba7730",  "created": "2022-11-28T00:00:00.000Z",  "name": "PAP:WHITE",  "extensions": {  "extension-definition-- f8d78575-edfd-406e-8e84-6162a8450f5b": {  "extension\_type": "property-extension",  "pap": "clear"  }  }  } |
| green | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--- c43594d1-4b11-4c59-93ab-1c9b14d53ce9",  "created": "2022-11-28T00:00:00.000Z"  "name": "PAP:GREEN",  "extensions": {  "extension-definition-- f8d78575-edfd-406e-8e84-6162a8450f5b": {  "extension\_type": "property-extension",  "pap": "green"  }  }  } |
| amber | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--- 60f8932b-e51e-4458-b265-a2e8be9a80ab",  "created": "2022-11-28T00:00:00.000Z"  "name": "PAP:AMBER",  "extensions": {  "extension-definition-- f8d78575-edfd-406e-8e84-6162a8450f5b": {  "extension\_type": "property-extension",  "pap": "amber"  }  }  } |
| red | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition-- 740d36e5-7714-4c30-961a-3ae632ceee0e",  "created": "2022-11-28T00:00:00.000Z",  "name": "PAP:RED",  "extensions": {  "extension-definition-- f8d78575-edfd-406e-8e84-6162a8450f5b": {  "extension\_type": "property-extension",  "pap": "red"  }  }  } |

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

# Extension Definition Object for PAP

{

"id": "extension-definition-- f8d78575-edfd-406e-8e84-6162a8450f5b",

"type": "extension-definition",

"spec\_version": "2.1",

"name": "PAP",

"description": "This defines PAP as a STIX extension",

"created": "2022-11-28T00:00:00.000Z",

"modified": "2022-11-28T00:00:00.000Z",

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

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

"version": "1.0.0",

"extension\_types": [

"property-extension"

]

}