ATT&CK™ Navigator Layer File Format Definition

This document describes version 4.0 of the MITRE ATT&CK Navigator Layer file format. The ATT&CK Navigator stores layers as JSON, therefore this document defines the JSON properties in a layer file.

Property Table

Name	**Type**	**Required?**	**Default Value (if not present)**	**Description**
`versions`	Version object	No		See Version object definition below
`name`	String	Yes	n/a	The name of the layer
`description`	String	No	**“”**	A free-form text field that describes the contents or intent of the layer
`domain`	String	Yes	n/a	Technology domain that this layer represents. Valid values are: `enterprise-attack` `mobile-attack` `ics-attack`
`filters`	Filter object	No		See Filter object definition below
`sorting`	Number	No	`0`	Specifies the ordering of the techniques within each tactic category as follows: `0`: sort ascending alphabetically by technique name `1`: sort descending alphabetically by technique name `2`: sort ascending by technique score `3`: sort descending by technique score

Name	Type	Required?	Default Value (if not present)	Description
`Layout`	Layout object	No		See definition of Layout object below
`hideDisabled`	Boolean	No	`false`	Specifies whether techniques that have been disabled are still displayed (greyed-out) or omitted from the view as follows: `true`: omit techniques marked as disabled from the view `false`: include disabled techniques in the view but display as greyed-out
`techniques`	Array of Technique objects	No		See definition of Technique object below.
`gradient`	Object	No	Red to Green, `minValue`= 0, `maxValue`= 100	
`legendItems`	Array of LegendItem objects	No		See definition of LegendItem object below
`showTacticRowBackground`	Boolean	No	`false`	If true, the tactic row background color will be the value of the tacticRowBackground field
`tacticRowBackground`	String	No	"`#dddddd`"	The tactic row background color

Name	Type	Required?	Default Value (if not present)	Description
`selectTechniquesAcrossTactics`	boolean	No	True	If true, selecting a technique also selects all instances with the same technique ID. See also selectSubtechniqueWithParent
`selectSubtechniquesWithParent`	boolean	No	True	If true, selecting a technique will also select all subtechniques of the technique. See also selectTechniqueAcrossTactics
`metadata`	Array of Metadata objects	No		User defined metadata for this layer. See definition of Metadata object below

Technique Object Properties

Technique objects are used to store both techniques and subtechniques. The only difference in representation between a technique and a subtechnique is in the techniqueID field, which for subtechniques is the parent technique ID followed by the subtechnique-id suffix.

Name	Type	Required?	Default Value (if not present)	Description
`techniqueID`	String	Yes	n/a	Unique identifier of the ATT&CK technique, e.g. "T####". For subtechniques, the format is "T####.###", where the substring to the left of the decimal is the parent technique ID, and the right-side substring is the subtechnique ID suffix.
`tactic`	String	No	n/a	Unique identifier of the ATT&CK technique's tactic, e.g. "lateral-movement". If the field is not present, the annotations for the technique will appear under every tactic the technique belongs to
`comment`	String	No	""	Free-text field
`enabled`	Boolean	No	`true`	Specifies if the technique is considered enabled or disabled in this layer
`score`	Number	No	(unscored)	Optional numeric score assigned to this technique in this layer. If omitted, the technique is consider to be "unscored" meaning that it will not be assigned a color from the gradient by the Navigator.
`color`	String	No	""	Explicit color value assigned to this technique in this layer. Note that explicitly defined color overrides any color implied by the score – the Navigator will display the technique using the explicitly defined color.

Name	Type	Required?	Default Value (if not present)	Description
`metadata`	Array of Metadata objects	No		User defined metadata for this technique. See definition of Metadata object below

Gradient Object Properties

Name	Type	Required?	Default Value (if not present)	Description
`colors`	Array of string	Yes	n/a	Specifies the hexadecimal RGB color values that constitute the color spectrum in use. The array must contain at least two (2) values, corresponding to the minValue and maxValue scores.
`minValue`	Number	Yes	n/a	The lower bound score of the gradient.
`maxValue`	Number	Yes	n/a	The upper bound score of the gradient. Note: maxValue must be > minValue

LegendItem Object Properties

Name	Type	Required?	Default Value (if not present)	Description
`label`	String	Yes	n/a	The name of the legend item
`color`	String	Yes	n/a	The color of the legend item

Metadata Object Properties

Name	Type	Required?	Default Value (if not present)	Description
`name`	String	Yes	n/a	The name of the metadata
`value`	String	Yes	n/a	The value of the metadata

Layout Object Properties

Name	Type	Required?	Default Value (if not present)	Description
`layout`	String	No	"`side`"	The layout of the matrix. Either "`side`", "`flat`" or "`mini`"
`showID`	Boolean	No	`false`	If true, show the ATT&CK ID of techniques and tactics in the matrix
`showName`	Boolean	No	`true`	If true, show the name of the techniques and tactics in the matrix

Filter Object Properties

Name	Type	Required?	Default Value (if not present)	Description

`platforms`	Array of string	No	All platforms within domain	Specifies the platforms within the technology domain – only those techniques tagged with these platforms are to be displayed. Valid values are as follows:
				
				`domain=enterprise-attack: PRE, Windows, Linux, macOS, Network, AWS, GCP, Azure, Azure AD, Office 365, SaaS`
				
				`domain=mobile-attack: Android, iOS`
				
				`domain=ics-attack: Windows, Control Server, Data Historian, Engineering Workstation, Field Controller/RTU/PLC/IED, Human-Machine Interface, Input/Output Server, Safety Instrumented System/Protection Relay`

Version Object Properties

Name	Type	Required?	Default Value (if not present)	Description
`attack`	String	No	Current version of ATT&CK: "`8`"	ATT&CK version of this layer.
`navigator`	String	Yes		Must be "`4.0`"
`layer`	String	Yes		Must be "`4.0`"

Example

The following example illustrates the layer file format:


```
{
   "name": "example layer",
   "versions": {
         "attack": "8",
         "navigator": "4.0",
         "layer": "4.0"
   },
   "domain": "enterprise-attack",
   "description": "hello, world",
   "filters": {
      "platforms": [
         "Windows",
         "macOS"
      ]
   },
   "sorting": 2,
   "layout": {
      "layout": "side",
      "showName": true,
      "showID": false
   },
   "hideDisabled": false,
   "techniques": [
      {
         "techniqueID": "T1110",
         "color": "#fd8d3c",
         "comment": "This is a comment for technique T1110",
         "showSubtechniques": true
      },
      {
         "techniqueID": "T1110.001",
         "comment": "This is a comment for T1110.001 - the first subtechnique of technique T1110.001"
      },
      {
         "techniqueID": "T1134",
         "tactic": "defense-evasion",
         "score": 75,
         "comment": "this is a comment for T1134 which is only applied on the defense-evasion tactic"
      },
      {
         "techniqueID": "T1078",
         "tactic": "discovery",
         "enabled": false
```

```
        },
        {
          "techniqueID": "T1053",
          "tactic": "privilege-escalation",
          "metadata": [
            {
              "name": "T1053 metadata1",
              "value": "T1053 metadata1 value"
            },
            {
              "name": "T1053 metadata2",
              "value": "T1053 metadata2 value"
            }
          ]
        }
    ],
    "gradient": {
      "colors": [
        "#ff6666",
        "#ffe766",
        "#8ec843"
      ],
      "minValue": 0,
      "maxValue": 100
    },
    "legendItems": [
      {
        "label": "Legend Item Label",
        "color": "#FF00FF"
      }
    ],
    "showTacticRowBackground": true,
    "tacticRowBackground": "#dddddd",
    "selectTechniquesAcrossTactics": false,
    "selectSubtechniquesWithParent": false,
    "metadata": [
      {
        "name": "layer metadata 1",
        "value": "layer metadata 1 value"
      },
      {
        "name": "layer metadata 2",
        "value": "layer metadata 2 value"
      }
    ]
}
```