MISP OBJECT TEMPLATE

BUILDING CUSTOM AND OPEN DATA MODELS

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/ TWITTER: @MISPPROJECT

NSPA



MISP Object Template



Objects - or How We Learned to Stop Worrying and Love the Templates

- Attributes are a simple but powerful tool to describe data
- Lacking the capability to create containers around attributes describing a common concept
- The goal was to develop something semi-standardised, with the option to dynamically build templates
- We have considered a list of different solutions such as simple boolean operators, but found that the current implementation was superior.
- The result is a simple template that uses the basic attriubte types as building blocks along with some meta data
- The template does not have to be known in order to use the constructed objects
- What we maintain now is a set of common objects, but similarly to our other JSON formats, users can extend it with their own ideas.

MISP Object Template

05

8 8 0

2022-

└─Objects - or How We Learned to Stop Worrying and Love the Templates OBJECTS - OR HOW WE LEARNED TO STOP WORRYIN AND LOVE THE TEMPLATES

- Attributes are a simple but powerful tool to describe data
 Lacking the capability to create containers around attribute describing a common correct
- The goal was to develop something semi-standardised, with the option to dynamically build templates
- We have considered a list of different solutions such as simple boolean operators, but found that the current
- implementation was superior. The result is a simple template that uses the basic
- types as building blocks along with some meta data The template does not have to be known in order to use the constructed objects
- What we maintain now is a set of common objects, but similarly to our other JSON formats, users can extend it with their own ideas

MISP OBJECT TEMPLATES

- Using a similar JSON format as the taxonomies, galaxies, warninglists.
- You can find the default set of object templates in the git repository¹.
- Some of the object templates capture objects from other standards or mimic the output of tools
- We tried to capture the most common use-cases coming from our own use-case as well as those of various partners that got involved
- Improvements or pull requests for new object templates are of course always welcome

MISP Object Template

05

2022-08

- Using a similar ISON format as the taxonomies, galaxies, warningits:
 You can find the default set of object templates in the git repositor)¹.
 Some of the object templates capture objects from other standards or minimic the output of tools
 We tried to capture the most common use-cases coming from our own use-cases as well as those of various partners
- that got involved Improvements or pull requests for new object templates are

ttps://www.github.com/MISP/misp-objects

https://www.github.com/MISP/misp-objects/

EXISTING OBJECT EXAMPLES

- AIL-leak AIL object, an example for an object catering to the output of another tool
- Android permission An object used to further contextualise another object
- Bank account
- File Generic object to describe a file
- Passive DNS
- Regex
- Sandbox report
- Vulnerability Enabling new use-cases such as pre-sharing of vulnerability information
- **X509**
- Yara Verbatim sharing of rule sets along with meta-data

MISP Object Template

05

8 8 0

2022

Existing Object examples

EXISTING OBJECT EXAMPLES

 Al-Vice-X. As object, an example of two object cateling to be endpared attached tool.
 An object, and another tool.
 An object cateling the object cateling

OBJECT TEMPLATE SKELETON

ہ MISP Object Template

80 2022

└─Object Template skeleton

TEMPLATE SKELETON	

1 "requiredOneOf": [], 2

- "required": [],
- "attributes": {},
- "version": 1, 5
- "description": "My description", 6
- "meta-category": "Chosen meta category",
- "uuid": "Object template uuid", 8
- "name": "Object template name" 9
- 10

ADDING ELEMENTS TO AN OBJECT TEMPLATE

ADDING ELEMENTS TO AN OBJECT TEMPLATE

မ္မ MISP Object Template

2022-08

Adding elements to an object template

	"regesp-type": { "description": "Type of the regular expression syntax.";
	"disable correlation": true.
2	"ui-priority": o,
ŝ	"minp-attribute": "text", "values list": [
2	"PCRE".
5	"POSIX BRS"
	"POSIX ERE"

1 "regexp-type": {

- 2 "description": "Type of the regular expression syntax.",
- 3 "disable_correlation": true,
- 4 "ui-priority": o,
- 5 "misp-attribute": "text",
- 6 "values_list": [
- "PCRE",
- 8 "PCRE2",
- 9 "POSIX BRE",
- 10 "POSIX ERE"
- 11
- 12 },

ATTRIBUTE KEYS

- Primary key: Object relation
- description: A description of the attribute in relation to the object
- disable_correlation: You can disable correlations for attributes in the resulting object
- ui-priority: Not implemented yet, but the idea is to have a "quick view" of objects only showing certain prio levels
- misp-attribute: The misp attribute type used as as the building block
- values_list: an optional list of values from which the user
 must choose instead of entering a value manually
- sane_defaults: an optional list of values from which the user may choose instead of entering a value
- multiple: Allow the user to add more than one of this attribute

می MISP Object Template مجمع المحافظ MISP Object Template ATTRIBUTE KEY

- Primary key: Object relation
- description: A description of the attribute in relation to the object
- disable_correlation: You can disable correlations for attributes in the resulting object
- ui-priority: Not implemented yet, but the idea is to have a "ouick view" of objects only showing certain prio levels
- misp-attribute: The misp attribute type used as as the building block
- walues_list: an optional list of values from which the user must choose instead of entering a value manually
- sane_defaults: an optional list of values from which the use may choose instead of entering a value
- multiple: Allow the user to add more than one of this attribute

හ MISP Object Template

8 8 0

2022

Enforcement of certain keys

- The template also defines which of the added attributes are mandatory
- Requirements are pointed to via their object relations name
- We differentiate between two types of rule sets:
 Required: Everything in this list has to be set in order for the
- object to validate Required One Of: Any of the attributes in this list will satisfy

- The template also defines which of the added attributes are mandatory
- Requirements are pointed to via their object relations names
- We differentiate between two types of rule sets:
 - Required: Everything in this list has to be set in order for the object to validate
 - Required One Of: Any of the attributes in this list will satisfy the requirements

WHAT WILL THE TEMPLATE ACTUALLY DO?

2022-08-05

MISP Object Template

└─What will the template actually do?

Templates create a form that can be used to populate an event

- When using templates, MISP will enforce everything
- according to the template rules
- However, these are only optional, users can avoid using the templates when creating events via the API
- The reason for this is that you do not need to have the
- template in order to create an object The limitation of this system: You cannot modify objects that
- The unitation of this system: You cannot mouny objects in were created with unknown templates

- Templates create a form that can be used to populate an event
- When using templates, MISP will enforce everything according to the template rules
- However, these are only optional, users can avoid using the templates when creating events via the API
- The reason for this is that you do not need to have the template in order to create an object
- The limitation of this system: You cannot modify objects that were created with unknown templates

TEMPLATES AS RENDERED IN THE UI

Add File Object

Object	Template	File v10					
Descri	ption	File object describing a file with meta-information					
Requir	Requirements Required one of: filename, size-in-bytes, authentihash, ssdeep, imphash, pehash, md5, sha1, sha224, sha256, sha384, sha512						
		sha512/224, sha	a512/256, tlsh, pa	attern-in-file, x509-fingerprint-sha	1, malware-sample		
Meta c	ategory	File					
Distrib	ution	Inherit event	t	v			
Comment					4		
Save	Name :: type		Description	Category	Value		
ouro	itane ii type		Decemption	outogory			
	Md5 :: md5		[Insecure] MD5 hash	Payload delivery	Ŧ		
			(128 bits)				
	Pattern-in-file :: pattern-in-file		Pattern that	Payload installation	v		
			can be found				
			in the file				
Sha256 :: sha256			Secure Hash	Payload delivery	v		
			Algorithm 2	Payloau delivery	•		
			(256 bits)				
			Secure Hash				
	Sha512 :: sha512	iha512 :: sha512		Payload delivery	•		
			(512 bits)				
	Fileneme - filenen		Filonomo on	(

မှ MISP Object Template

2022-08

└─Templates as rendered in the UI

And File Ob	(rel						
		File staps description for with resident states and the states of the st					
and a second second	INVESTIGATION OF	ANE GOTA, MALIN	atere is the shift to provide the	1. Huhari sangir			
Determine							
Dave Plane 1 is		Description	Entropyce	Vote			
		(nemar) Michael (Little)	Papinal informy				
mente	Bergateria fe	months outstand is the fix	Paylost insulation				
i inde	ACR.	Journ Rah Agaited Gilling	Paylot belowy				
-	Arita I	Anan Kali Anathin 2	Papinel Anterry				

TEMPLATES AS RENDERED IN THE UI

MISP Object Template

└─Templates as rendered in the UI

		 ٠
		٠
	-	 ٠

	2018-03-27	Name: No 🖍 References: 1 🖍	•		
8	2018-03-27	Payload delivery	filename: filename	putty.exe	•
8	2018-03-27	Other	size-in-bytes: size-in-bytes	774200	0
8	2018-03-27	Other	entropy: float	6.7264597226	٥
8	2018-03-27	Payload delivery	md5: md5	b5c12d88eeb910784d75a5e4d954001	
8	2018-03-27	Payload delivery	shal: shal	5e19515e81d92x254dd2dcdd9c4b50x1x8007b8f	
8	2018-03-27	Payload delivery	sha256: sha256	81de431907304676134130705k1c21108ad7k27edf6b77a6551aa6931944 85e	0
8	2018-03-27	Payload delivery	sha512: sha512	e174ec44Th38d30c2ec68b3718287764212446124d5c913912e0f37385332b 7d107d5ac5bd19cb7Mdcdbd88b50664881aa30064e9610M213970c163cca7 8	0
	2018-03-27	Payload delivery	mahvare-sample:	puty.exe	



MISP Threat Sharing HITS://SIHub.com/HISP/HISP
 HITS://SIHub.com/HISP/HISP
 HITS://SIHub.com/HISP/HISP.objects
 HitSP://SiHub.com/HISP/HISP.objects
 HitSP://SiHub.com/HISP/HISP.objects
 HitSP://SiHub.com/HISP/HISP.objects
 HISP.objects
 H

- https://github.com/MISP/MISP
- https://github.com/MISP/misp-objects
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 CO02 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5