

MISP Threat Intelligence Summit 0x04

MISP42SPLUNK

A Splunk App to work with MISP

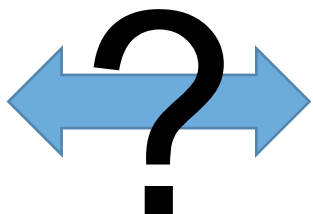
<https://github.com/remg427/>

Remi SEGUY

Disclaimer: I am not a developer, code is “as-is”

A bit of context...and a challenge.

Splunk Indexer



- Several interesting logs in Splunk: dns, proxy, email, ids, ...
- So many events and attributes that could be used.
- Option 1: CSV files
 - Manual, scheduled scripts, etc.
 - Not flexible
- Option 2: make a Splunk App

Thanks @XME! <https://blog.rootshell.be/2017/10/31/splunk-custom-search-command-searching-misp-iocs/>

MISP42SPLUNK: an App easy to install

- 1) Install Python3
- 2) Install PyMISP > 2.4.95
- 3) Download
<https://github.com/remg427/misp42splunk/blob/master/misp42splunk.tar.gz>
- 4) Splunk > Manage App > Install app from file
- 5) Restart Splunk
- 6) Splunk > Manage App > App-MISP42 > Set up
 - MISP URL
 - MISP authentication key
 - verify certificate?

MISP42SPLUNK – screen shots

Define MISP server parameters

Name ▾	Folder name ▾	MISP url:	Status ▾	Actions
App-MISP42	misp42splunk	https://misp.local	Enabled	Set up Launch app

Set the MISP auth key

Check SSL certificate of MISP server

(Optional) system path for Python3

Python3 binary path (default: /usr/bin/python3)

(Optional) Define TheHive server parameters

TheHive API url:

API auth key - You should create an account with only the role create alerts

MISP to Splunk – Custom Reporting command

- Use cases:
 - get IOC and update lookup tables
 - Get IOC and retro-hunt in logs
- Custom reporting command ==> first on the search line
 - Search:
| mispgetioc <params>
 - Subsearch:

```
|mispgetioc ( [eventid=id] | [last=interval] )  
  [onlyids=y|n]  
  [category="CSV_string"]  
  [type="CSV_string"]  
  **[getuuid=y|n|Y|N|0|1]**  
  **[getorg=y|n|Y|N|0|1]**  
  **[tags="CSV_string"]**  
  **[not_tags="CSV_string"]  
  [mispsrv=https://host:port]  
  [mispkey=misp-authorization-key]  
  [sslcheck=y|n]
```

MISP to Splunk – Custom Reporting command

- simple example

```
| misp42splunk last=1d
```

- update a lookup table

```
| misp42splunk last=1d type=domain | outputlookup domain.csv
```

- retro hunting

```
index=dns
```

```
[ |mispgetioc last=24h onlyids=1 type="domain"  
  |rename value AS dns_request_queried_domain  
  |fields dns_request_queried_domain]
```

```
|stats count AS total by dns_request_queried_domain
```

MISP for SPLUNK – alerts actions



Create events in MISP ready to publish



Increment sighting counters

Type 0 = sighting

Type 1 = false positive

 **TheHive** Bonus: create alerts in TheHive

Alerts actions: Create events in MISP ready to publish



- Make a search
| table _time to_ids eventkey info
category misp_* fo_* eo_* no_*
(etc.)
- Set an action

Global event parameters

Unique ID	<input type="text"/>	A field name that contains a unique identifier per event to be created. The default Info field for the MISP events if not provided in results.
Info	<input type="text" value="\$description\$"/>	
Distribution	<input type="text" value="Connected communities"/>	Change the Distribution. Defaults to Your organisation only
Threat Level	<input type="text" value="Low"/>	Change the Threat Level. Defaults to Undefined
Analysis	<input type="text" value="Complete"/>	Change Analysis status. Default to Initial
TLP	<input type="text" value="Green"/>	Change the TLP of the created alert. Defaults to TLP-Amber
Tags	<input type="text"/>	Use single comma-separated string without quotes for multiple tags (ex. "badIP,spam").

Specific MISP instance (overwrite general settings)

URL	<input type="text"/>	MISP URL (leave blank to use default settings).
Auth Key	<input type="text"/>	The Authkey to submit alerts to (leave blank to use default settings).
Check SSL	<input type="checkbox"/>	Check SSL certificate of MISP

Alert to create MISP event(s) Remove

Alert overall description

Title	<input type="text" value="test_creation"/>	The title of this alert.
Description	<input type="text" value="test description"/>	The description to send with the alert.

Alerts actions: Create events from sandbox report

```
index=sandbox
| rex mode=sed field=_raw "s#\n# #g"
| eval eventkey=md5(src_user)
| dedup eventkey
| rename src_user AS eo_from
| eval alert_subject=spath(_raw,"alert.smtp-message.subject")
| eval eo_subject=replace(alert_subject,"\[WARNING.*\]", "")
| eval src_url=spath(_raw,"alert.src.url")
| eval eo_attachment=if(match(src_url,"^hxxp"), "", if(match(src_url,"^ehdr"), "", src_url))
| eval misp_url=if(match(src_url,"^hxxp"), replace(src_url,"hxxp","http"), "")
| eval fo_filename=spath(_raw,"alert.explanation.malware-detected.malware{}.original")
| regex fo_filename!="ehdr$" | where isnotnull(fo_filename) OR isnotnull(misp_url)
| eval fo_md5=spath(_raw,"alert.explanation.malware-detected.malware{}.md5sum")
| eval fo_sha256=spath(_raw,"alert.explanation.malware-detected.malware{}.sha256")
| eval misp_domain=spath(_raw,"alert.explanation.malware-detected.malware{}.domain")
| eval misp_address=spath(_raw,"alert.explanation.cnc-services.cnc-service{}.address")
| eval misp_hostname=mvdedup(address)
| eval info=if(isnotnull(fo_filename),"malspam with attachment","malspam")
| mvexpand hostname
| table eventkey _time info action eo_from eo_subject eo_attachment misp_url misp_domain misp_hostname fo_filename fo_md5 fo_sha256
```

Alerts actions: Sighting on attributes

👍 👎 🔧
(1/0/0)

- Mode 1: by values
 - Make a search with
 - as many fields as you like
 - and a timestamp field.

```
index=email
| dedup sender
| search [ | mispgetioc last=1d type=email-src
| where type="email-src"
| rename value AS sender
| fields sender ]
| rename message_subject AS email_subject, file_name AS filename
| table _time mid sender mail_subject filename value
```

- Mode 2: by uuid
 - Make a search which includes uuid

Alert for sighting MISP attribute(s) Remove

Alert overall description

Title The title of this alert.

Description The description to send with the alert.

Global event parameters

Unique ID A field name that contains timestamps (_time, stptime() etc.). If not defined or not set mode for sighting. Default present, default to now() to "matching values"

Mode Set mode for sighting. Default present, default to now() to "matching values"

Type Set type of sighting

Specific MISP instance (overwrite general settings)

URL MISP URL (leave blank to use default settings).


Auth Key The Authkey to submit alerts to (leave blank to use default settings).

Check SSL Check SSL certificate of MISP server.

Alerts actions: Alerts in TheHive



- Set an action

▼  create THEHIVE alert(s) (alert action) Remove

- Define parameters

- (optional) point to another instance

TheHive API parameters (optional if they have been defined in general setup)

URL The URL to submit alerts to e.g. <http://hive.example.com/api/alert>.

API KEY The API KEY for authentication

Alert overall description

Case Template	<input type="text"/>	The case template to use for imported alerts.
Type	<input type="text" value="alert"/>	The alert type. Defaults to "alert".
Source	<input type="text" value="splunk"/>	The alert source. Defaults to "splunk".
Unique ID	<input type="text"/>	A field name that contains a unique identifier specific to the source event.
Title	<input type="text" value="\$name\$"/>	The title to use for created alerts.
Description	<input type="text" value="\$description\$"/>	The description to send with the alert.
Tags	<input type="text"/>	Use single comma-separated string without quotes for multiple tags (ex. "badIP,spam").
Severity	<input type="text" value="Low"/>	Change the severity of the created alert.
TLP	<input type="text" value="TLP:AMBER"/>	Change the TLP of the created alert. Default is TLP:AMBER

MISP42SPLUNK – Custom Streaming command

- Work in Progress for v4
- Use cases:
Get MISP info on matching values
 - misp_json
 - misp_type
 - misp_value
 - misp_to_ids
 - misp_category
 - misp_uuid
 - misp_event_id
 - misp_comment

search something...

```
| mispquery field=<a_field>
```

```
[onlyids=y|n]
```

```
[get_comment=y|n]
```

```
[mispsrv=https://host:port]
```

```
[mispkey=misp-authorization-key]
```

```
[sslcheck=y|n]
```