FORTINET

KNOWLEDGE GUIDE – ADVANCED USERS

FortiSIEM

Integrating with MISP

Importing Threat Intelligence IOC from MISP into the FortiSIEM CMDB.

US ATP Team

March 2020

Introduction

Purpose and Scope

FortiSIEM is advanced Security Information Event Management system which incorporates an event database (proprietary NoSQL or elastic search database) with a CMDB postgreSQL database. Both databases are utilized in terms of analytics (search/reporting/dashboarding) and event correlation, with the CMDB categorizing nearly 200,000 unique multi-vendor events into functional correlation categories.

MISP (Malware Information Sharing Project) is an Open Source Threat Intelligence Platform and a community-driven project - www.misp-project.org. What MISP provides amongst many things is an **IOC** and **indicators** database allowing users to store technical and non-technical information about malware samples, incidents, attackers and intelligence.

The purpose of this FortiSIEM integration is to currently query MISP and produce a list of indicators to populate into the FortiSIEM CMDB threat related containers.

Disclaimer

When mentioned in this document and this document only, the following terms and definitions will apply:

- This document and provided script are provided as is, and may not be 100% accurate use caution.
- The script is designated as an internal/PoV usage script and hence is designed without error checking or resource restraints and hence **should only be used on a test/PoV system only**.
- TAC is not expected to support this script.
- Usage of this script is at your own risk.
- Any questions should be posted via FUSE or FNDN or directly to cdurkin@fortinet.com

Usage

Installing the MISP script

In addition to this document a file name **fsmMISPIntegration.zip** should also have also been provided.

Create a new directory for this program under the /root directory for example *MISP* on your FortiSIEM test environment and then copy this file via WinSCP/Cyberduck or favourite secure copy program to this directory, where it should be unzipped and then executed.

For example, this process can be obtained via the commands below.

```
mkdir MISP
cd MISP
unzip fsmMISPIntegration.zip
chmod +x fsmMISP.sh
```

Before Running the MISP script for the first time.

The fsmMISP script has some pre-requites that need populating before running the script. Use Vi or similar to define your MISP API Key and Server IP details along with the IP Address of your FortiSIEM Supervisor node.

```
#Enter your MISP API Key and Server Details
MISP_APIKEY="<enter here>"
MISP_SERVER="<enter here>"

#Enter your FSM Server IP
FSM_IP="<enter here>"
```

Understanding the MISP script components.

The fsmMISP script provides some query JSON files in the same directory it is extracted. These files are related to the indicator types than can be imported into FortiSIEM, and each provides a custom query to extract this data from your MISP platform.

For example looking at the file misp_url_query.json :

```
{
      "request": {
            "type": "url",
            "category": "Network activity",
            "last": "1d",
            "enforceWarninglist": "True"
      }
}
```

The type in this case is **url** for the last **1 day**. These files are customizable, for example the time can be set to 5**d** or 12**h** or 30**m** etc.

Each file has a separate query for the following data:

File Name	Description
misp_domain_query.json	DNS Domains
misp_hashes_query.json	MD5, SHA1 and SHA256 Hashes
misp_ip_query.json	Source and Destination IP
misp_md5_query.json	Only MD5 Hashes
misp_sha1_query.json	Only SHA1 Hashes
misp_sha256_query.json	Only SHA256 Hashes
misp_url_query.json	URL IOC

MISP Script Output

The fsmMISP script uses the MISP API to make one or more queries and grab the resultant IOC data as JSON, which is then formatted and relevant fields are converted to CSV format for import into FortiSIEM.

An example of the converted output for URL is as below:

```
#URL,Malware Type,Description,Last Seen
"http://soheylistore.ir:80:/modules/mod_feed/feed.php","OSINT - Carbon Paper:
Peering into Turla's second stage backdoor","C&C server addresses (hacked websites
used as 1st level of proxies","2017-03-30 02:54PM"
```

Preparing your FortiSIEM for MISP IOC Data

The fsmMISP script is expected to be run locally on your FortiSIEM Supervisor and the CSV data written to a local folder that the FortiSIEM can reach for import (ie: itself). In production this could run on a different machine, with a 3rd party URL used for accessing the data.

Prepare the Supervisor

From an SSH session, create a new directory on the Supervisor as follows:

```
mkdir /var/www/html/ioc
```

This is the location that the fsmMISP script will dump its CSV files ready for import.

Prepare the FortiSIEM GUI

Within the FortiSIEM Resources Tab under the various Threat Intel categories, create a folder for the MISP data.

For example, the following folders could be created: (names are not important)

Parent Folder	Custom Folder
Malware URLs	MISP URL
Malware IPs	MISP IP
Malware Domains	MISP Domain
Malware Hash	MISP MD5 etc..

Running the MISP script

Execute the MISP script from the extracted directory via one of the two methods below.

```
./fsmMISP.sh <options>
Or
./fsmMISP.sh
```

The <*options*> above are one or more comma separated entries as per the table below.

Once the script completes the output (CSV files) are created under the **/var/www/html/ioc** folder.

Option	Description
url	MISP URLS returned via misp_url_query.json
md5	MISP MD5 returned via misp_md5_query.json
sha1	MISP SHA1 returned via misp_sha1_query.json
sha256	MISP SHA256 returned via misp_sha256_query.json
hashes	MISP MD5,SHA1 & SHA256 hashes returned via misp_hashes_query.json
domain	MISP DOMAINS returned via misp_domain_query.json
ip	MISP Source and Destination IP returned via misp_ip_query.json
NULL (ie: no option specified)	ALL MISP Queries above are performed

Examples

```
# Collect MISP md5, ip and urls
./fsmMISP.sh md5,ip,url

# Collect MISP sha1 hashes only
./fsmMISP.sh sha1
```

The script can be scheduled to run every so often via a cron job on the FortiSIEM backend.

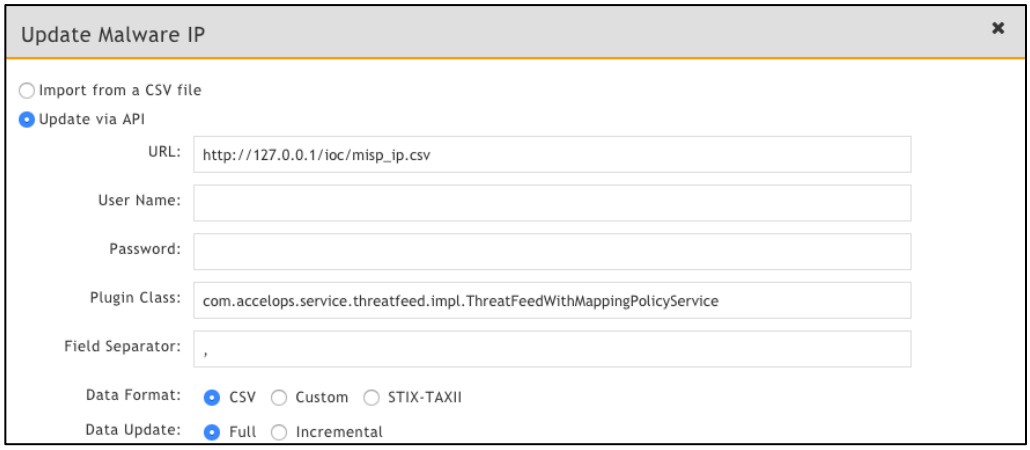
Scheduling FortiSIEM to Populate the CMDB with IOC Data

Once the CSV files are ready, they can be imported (and scheduled if required) via the GUI under the Resources Tab.

Malware IP

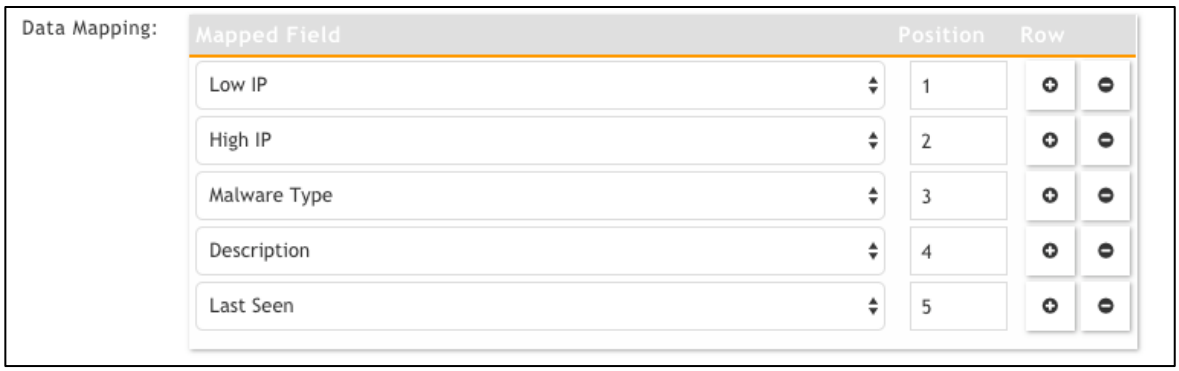
Navigate and then select to the custom **MISP IP** folder previously created, then select **More -> Update**.

Choose the option to **Update via API** and then click the pencil option and populate the **URL** as **http://127.0.0.1/ioc/misp_ip.csv**



Notice here the **Data Update** options for Full or Incremental updates.

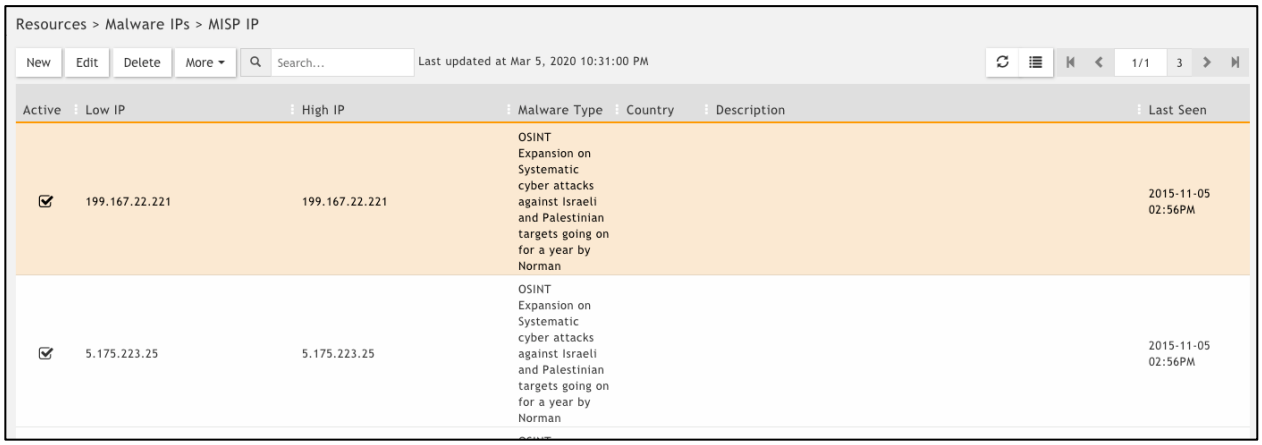
For the Data Mapping for the CSV file, define the following:



Then click **Save**.

Then click the plus icon against schedule and set a time / recurrence pattern as necessary and then click **Save** and **Done** when completed.

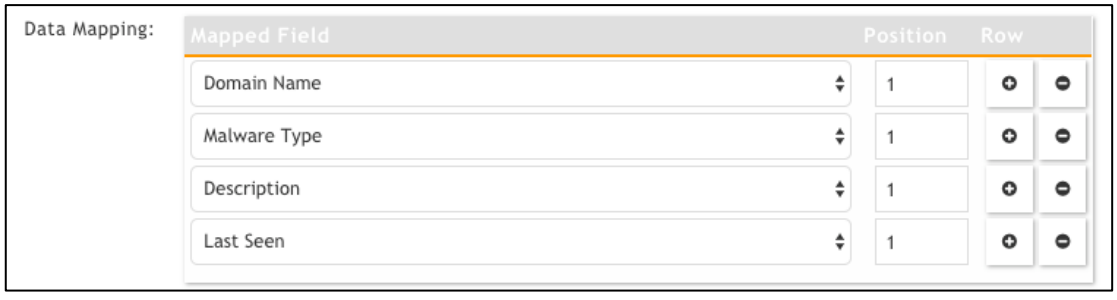
Once the schedule is met, then the MISP IPs should be imported as below:



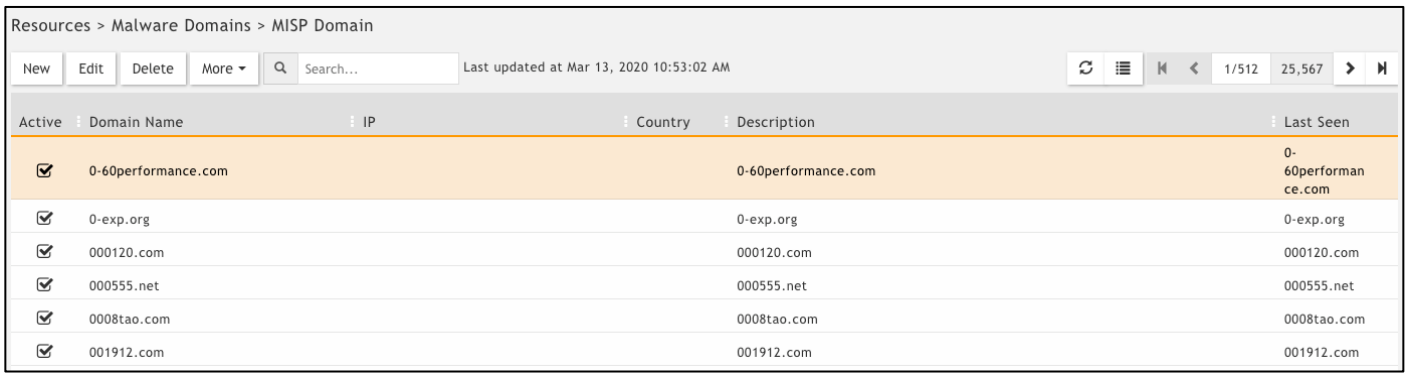
Malware Domain

For the MISP Domains, select the custom folder created earlier and again set to update via API, and this time use the following URL and Mappings and schedule as necessary.

URL: **http://127.0.0.1/ioc/misp_domain.csv**



Once the schedule is met, then the MISP Domains should be imported as below:



Active	Domain Name	IP	Country	Description	Last Seen
☑	0-60performance.com			0-60performance.com	0-60performance.com
☑	0-exp.org			0-exp.org	0-exp.org
☑	000120.com			000120.com	000120.com
☑	000555.net			000555.net	000555.net
☑	0008tao.com			0008tao.com	0008tao.com
☑	001912.com			001912.com	001912.com

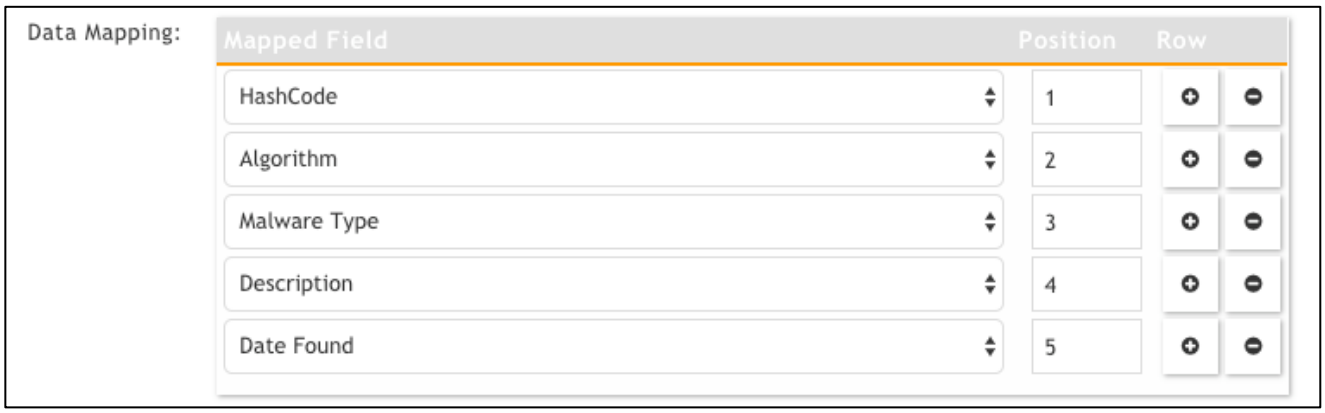
Malware Hashes

For the MISP **MD5, SHA1,SHA256** or the aggregated **Hashes** option (all formats together), select the custom folder or folders created earlier and again set to update via API, and this time use the following URL and Mappings and schedule as necessary.

Obviously, you only need to define the entries that you need.

URL for MD5: **http://127.0.0.1/ioc/misp_md5.csv**
URL for SHA1: **http://127.0.0.1/ioc/misp_sha1.csv**
URL for SHA256: **http://127.0.0.1/ioc/misp_sha256.csv**
URL for All Hashes: **http://127.0.0.1/ioc/misp_hashes.csv**

Mappings are the same for each type, and MD5 is shown below as an example:



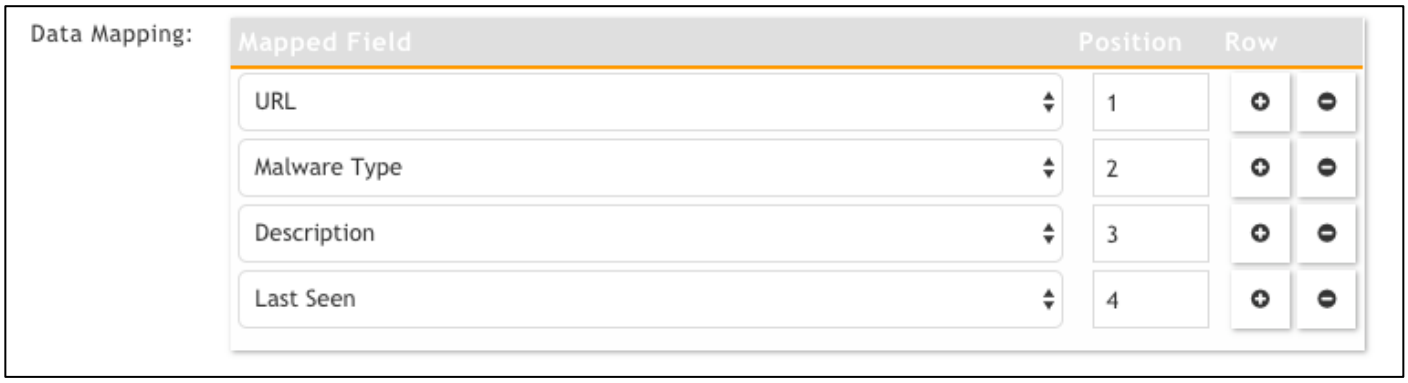
Once the schedule is met, the MISP MD5 should be imported as below:

Active	Botnet Name	Algorithm	Hash Code	Malware Type	Confidence	Country	Date Found
☑		MD5	42279796df60c183ccf29633a173d250	OSINT - Operation SMN (Novetta)			2014-11-05 02:24PM
☑		MD5	a344b9520f975d2cc827165fbd9f0073	SectorJ04 Group's Increased Activity in 2019			2019-09-04 03:02PM
☑		MD5	9476ed0a007ba332b7da0a657b1608bd	Import of CitizenLab public DB of malware indicators			2014-11-21 10:19AM
☑		MD5	d635e232a6ae94f2b273d16f5a0e90ff	OSINT Fidelis Threat Advisory #1018 Looking at the Sky for a DarkComet from the Fidelis Cybersecurity			2015-09-30 11:15AM

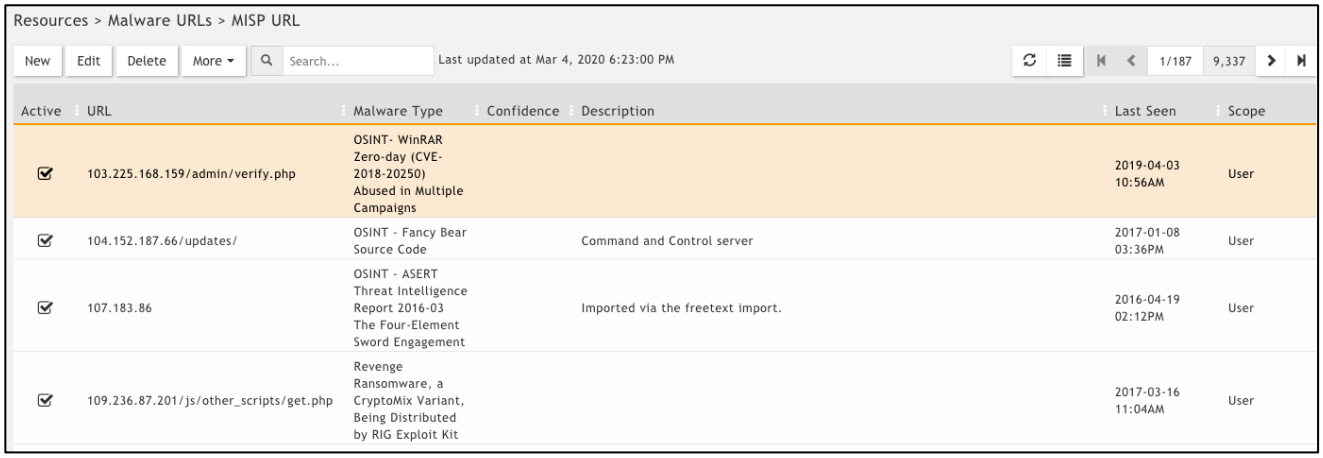
Malware URL

For the MISP URLs, select the custom folder created earlier and again set to update via API, and this time use the following URL and Mappings and schedule as necessary.

URL: **http://127.0.0.1/ioc/misp_url.csv**



Once the schedule is met, then the MISP URLs should be imported as below:



MISP script logging

Two logging options have been provided.

A) **misp_log.txt** log file in the current directory the script is run.

This records the results of the last time the script was run.

```
FSM MISP Last Run at Mar 13 20.45.56 2020
Process MD5
FSM : 30841 records ready for upload
```

B) **Syslog** to FortiSIEM

The script will send syslog messages to the IP address of your FortiSIEM.

A parser (misp_parser.xml) is in the directory where the script was extracted, which can be deployed. (The parser test message is within the parser).

Results will look like the following: