LTS Secure 4.5

Implementation Document for

Threat Intelligent Hub

Prepared by

Anurag Gundappa

Document Details

Project / Name	LTS Secure - SIEM
Current Version	1.0
List of Contributors	
Customer Contact Information	

Prepared by	Reviewed by	Approved by/Date
Anurag Gundappa	Priyanka Kuskar	

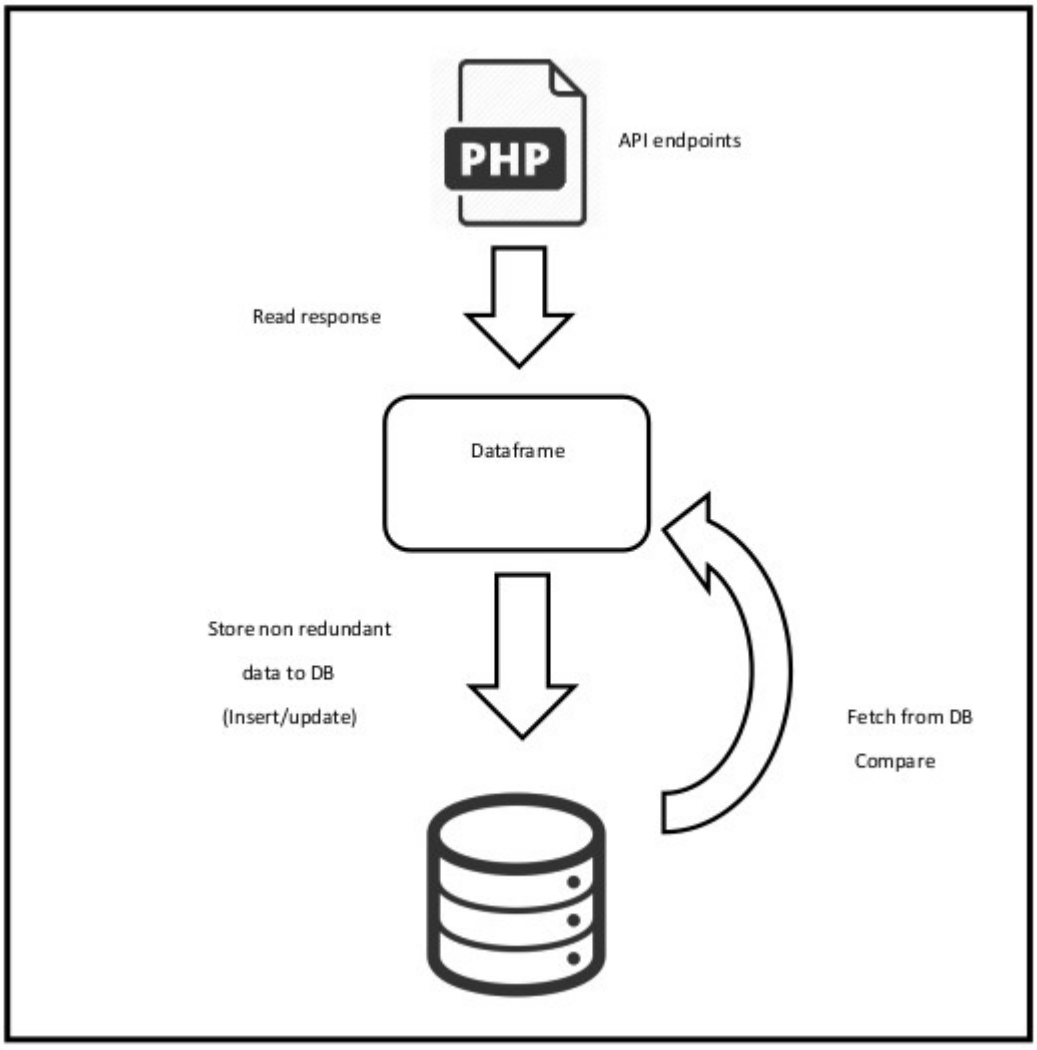
Revision History

Version	Date	Description of Change	Reason for Change	Affected Sections
1.0	18-11-2019	Draft		

Table of Content

Introduction/Background:

A system to store, collect and manage blocked IP address and Malicious URLs, collected from the various global databases. Threat intelligent hub is set of database and API to access these databases. This hub includes two modules namely IP address, Ransomware database and Malicious URLs database.



Purpose

This threat intelligent hub eliminates the need of Open Threat Exchange (OTX) which is currently integrated into LTS SIEM. Now LTS has its own threat database which is ever growing

in nature. It supports as much as possible threat data collected from real time threat databases on the internet.

LTS Secure – Feature details

The developed feature is database of two tables which is managed by a Python program. This program handles the database insertion and updation task.

There is also a set of APIs which are also written in Python Flask and hosted with domain **threatdb.leosys.net.**

The full list of API endpoints are as follows

1. threatdb.leosys.net/api/register
2. threatdb.leosys.net/api/ip/list
3. threatdb.leosys.net/api/ip/list?revision=<number>
4. threatdb.leosys.net/api/ip/search?ip=<ip-address>
5. threatdb.leosys.net/api/url/list
6. threatdb.leosys.net/api/url/list?threat_type=phishing
7. threatdb.leosys.net/api/url/list?threat_type=malware
8. threatdb.leosys.net/api/url/list?threat_type=ransomware
9. threatdb.leosys.net/api/url/list?domain=<domain>
10. threatdb.leosys.net/api/url/list?filename=<filename>
11. threatdb.leosys.net/api/url/search?url=<url>

Change in Files:

This newly developed feature does not directly related with SIEM therefore no changes in existing SIM code files. It is integrated with the help of API.

User Interface Details :

The developed threat hub does not have special UI. It is a database with python manager program (script) which only needs to be run periodically and two database table to manage data.

Deployment Environment Details:

- **SVN-repo:**
- http://172.16.0.20/centralised_t_intelligence/threat-intell-hub/
- **Deployment location:**
- 172.16.0.188/home/threat-intell-hub/

Database Details:

The threat database is a MySQL 5.7 database. The designed table structure are as follows

blocked_ips table

```
mysql> desc blocked_ips;
+----------------+--------------+------+-----+-------------------+----------------+
| Field          | Type         | Null | Key | Default           | Extra          |
+----------------+--------------+------+-----+-------------------+----------------+
| id             | int(11)      | NO   | PRI | NULL              | auto_increment |
| ip_address     | varchar(50)  | NO   | MUL | NULL              |                |
| reliability    | int(11)      | YES  |     | NULL              |                |
| priority       | int(11)      | YES  |     | NULL              |                |
| activity       | varchar(128) | YES  |     | NULL              |                |
| sub_category   | varchar(128) | YES  |     | NULL              |                |
| country        | varchar(128) | YES  |     | NULL              |                |
| city           | varchar(128) | YES  |     | NULL              |                |
| latitude       | double       | YES  |     | NULL              |                |
| longitude      | double       | YES  |     | NULL              |                |
| source         | varchar(128) | YES  |     | NULL              |                |
| target         | varchar(128) | YES  |     | NULL              |                |
| dest_port      | int(11)      | YES  |     | NULL              |                |
| last_online    | varchar(128) | YES  |     | NULL              |                |
| first_seen     | varchar(128) | YES  |     | NULL              |                |
| used_by        | varchar(128) | YES  |     | NULL              |                |
| reference_link | varchar(128) | YES  |     | NULL              |                |
| created_at     | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| updated_at     | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| revision       | int(11)      | YES  |     | NULL              |                |
+----------------+--------------+------+-----+-------------------+----------------+
20 rows in set (0.00 sec)
```

malware_urls table

```
mysql> desc malware_urls;
+-------------+--------------+------+-----+-------------------+----------------+
| Field       | Type         | Null | Key | Default           | Extra          |
+-------------+--------------+------+-----+-------------------+----------------+
| id          | int(11)      | NO   | PRI | NULL              | auto_increment |
| url         | varchar(512) | YES  | MUL | NULL              |                |
| domain      | varchar(256) | NO   |     | NULL              |                |
| filename    | varchar(256) | NO   |     | NULL              |                |
| file_type   | varchar(256) | NO   |     | NULL              |                |
| priority    | varchar(256) | NO   |     | NULL              |                |
| country     | varchar(256) | NO   |     | NULL              |                |
| url_status  | varchar(256) | YES  |     | NULL              |                |
| date_added  | varchar(256) | YES  |     | NULL              |                |
| threat_type | varchar(256) | NO   |     | NULL              |                |
| threat_tag  | varchar(256) | YES  |     | NULL              |                |
| created_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| updated_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
+-------------+--------------+------+-----+-------------------+----------------+
13 rows in set (0.01 sec)
```

client_details table

```
mysql> desc client_details;
+-------------+--------------+------+-----+-------------------+----------------+
| Field       | Type         | Null | Key | Default           | Extra          |
+-------------+--------------+------+-----+-------------------+----------------+
| ID          | int(11)      | NO   | PRI | NULL              | auto_increment |
| Client_Name | varchar(50)  | NO   |     | NULL              |                |
| Client_IP   | varchar(50)  | NO   |     | NULL              |                |
| Created_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| Updated_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| api_key     | varchar(512) | YES  |     | NULL              |                |
+-------------+--------------+------+-----+-------------------+----------------+
6 rows in set (0.00 sec)
```

revision_tracker table

```
mysql> desc revision_tracker;
+---------------+-----------+------+-----+---------------------+-----------------------------+
| Field         | Type      | Null | Key | Default             | Extra                       |
+---------------+-----------+------+-----+---------------------+-----------------------------+
| id            | int(11)   | NO   | PRI | NULL                | auto_increment              |
| last_revision | int(11)   | YES  |     | NULL                |                             |
| created_at    | timestamp | NO   |     | CURRENT_TIMESTAMP   | on update CURRENT_TIMESTAMP |
| updated_at    | timestamp | NO   |     | 0000-00-00 00:00:00 |                             |
+---------------+-----------+------+-----+---------------------+-----------------------------+
4 rows in set (0.00 sec)
```

Other Details

Project Directory and modules:

This includes the following directory structure

threat-intell-hub/
- **api/**
- **commom/**
  - config.py
  - crawler.py
  - logger.py
  - targets.py
  - threat_db.py
- **docs/**
- **ip_address/**
  - ipdriver.py
  - location_updator.py
  - processor.py
- **logs/**
  - threat_hub.log
- **resource/**
  - db_updater.sh
  - GeoLite2-City.mmdb
- **urls/**
  - driver.py
  - parser.py
  - processor.py

main.py
requirements.txt
README.md

Explaination:

1. api/:

2. common/:

This directory contains utilities which are required for all the modules such as

1. A URL crawler,
2. A logger of logging purpose,

3. targets module to contain source endpoints
4. threat_db is a Mysql database API for interacting with Mysql database.

3. Docs/:

This directory contains project documentation and necessary resources.

4. ip_address/:

IP address is a python package containing ip_address module and functionality. This code handle database comparison and storing logic.

5. Logs/

A directory to contain threat_hub.log file generated and updated by logger module on project each project run.

6. Resource/

A directory to contain IP address city geolocation database from Maxmind and a updater shell script to update the database using cron job.

7. Urls/

urls is a python package containing module and functionality. This code handle database comparison and storing logic

8. ipmain.py

The main python executing script for blocked IP address and ransomware module

9. urlmain.py

The main python executing script for malicious urls module

10. requirements.txt

All python project dependencies to be install with pip install -r requirements.txt