**LTS Secure 5.0**

Implementation Document for

**Threat Intelligent Hub**

**DELETION MODULE**

Prepared by

**Anurag Gundappa**

Document Details

|  |  |
| --- | --- |
| Project / Name | LTS Secure - SIEM |
| Current Version | 2.0 |
| List of Contributors |  |
| Customer Contact Information |  |

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

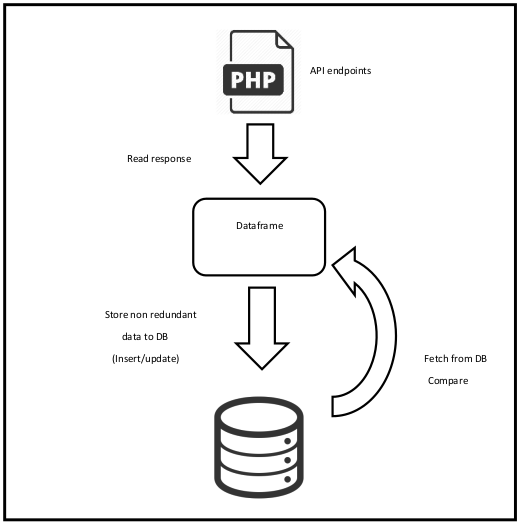
Revision History

| Version | Date | Description of Change | Reason for Change | Affected Sections |
| --- | --- | --- | --- | --- |
| 1.0 | 18-11-2019 | Threat-hub-completed |  |  |
| 2.0 | 23-12-2019 |  | New module developed | Purpose, Feature detail, Other details |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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**

The threat intell hub is alternative solution to the OTX. OTX does provide database version based on some condition. Somehow they have managing the updation of the IP data and they are incrementing the revision number containing the updated IP data.

This means that OTX is having some criteria of removing the IP data from their database. In other words the they are whit listing the IP address based on some condition. This scenario is encouraged us to define deletion condition for our IP address data.

By studying the behavior of sources from which we are currently fetching the IP and URL data, It is observed that they are storing IP blacklisted data for 48 hours only and then they update the database.

**LTS Secure – Feature details**

The feature adding only deletion logic to the existing code as an upgrade. Every time the threat intelligent hub will start with **run.sh** automatically, this same script will flush the database i.e. **blocked\_ips** and **malware\_urls** tables at first before inserting the data into these tables.

There is python class method which is going to execute at the start of the main logic. Which will actually do the work.

**Change in Files:**

This newly developed deletion feature does not directly related with SIEM therefore no changes in existing SIM code files. It is integrated with the help of API. It just need to run automatically at the rate of run per 48 hours with the help of cronjob.

**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.

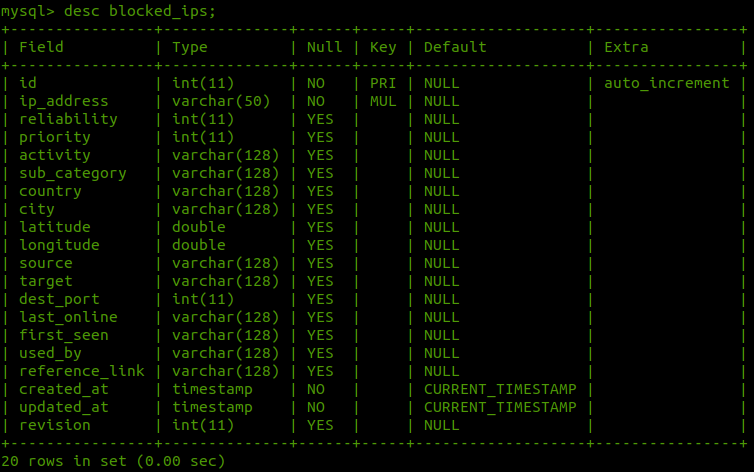
**Deployment Environment Details:**

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

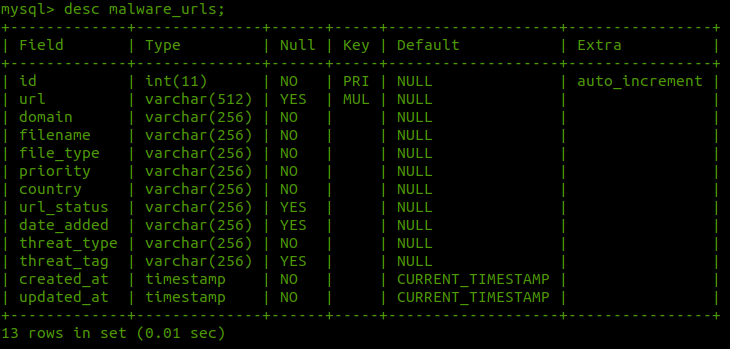
**Database Details:**

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

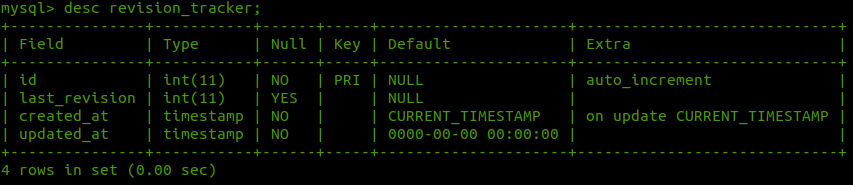
**blocked\_ips table**



**malware\_urls table**



**revision\_tracker table**



**Other Details**

**How to run?:**

1. Login to 172.16.0.188 host.
2. Go to home/home/ directory.
3. Access the threat-intell-hub/ folder.
4. Run the **run.sh** or **python3.6 main.py**.
5. Access the MySql database with **mysql -u dev -p.**
6. Access the logs in **threat\_hub.log** file.

**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**

**run.sh**

**db\_updator.sh**

**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. main.py**

The main python executing script for threat intelligent hub.

**9. run.sh**

This is shell script to be executed as a part of crontab automated task, which will trigger the main.py

**10. db\_updater.sh**

This script will update the IP gelocation database with updated data from **maxmind.com**

This script will get automatically once in a month.

**11. requirements.txt**

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