**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 |  |

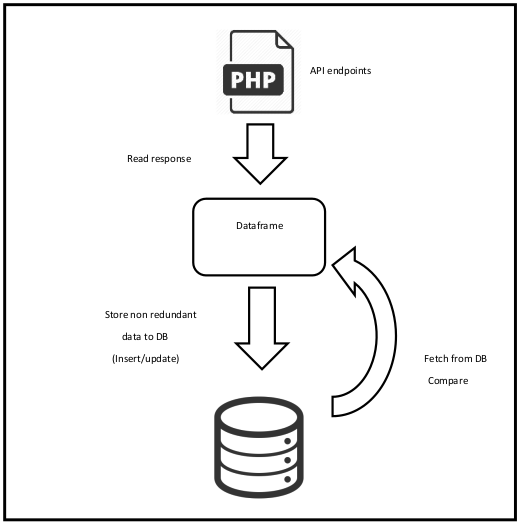
Revision History

| 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.

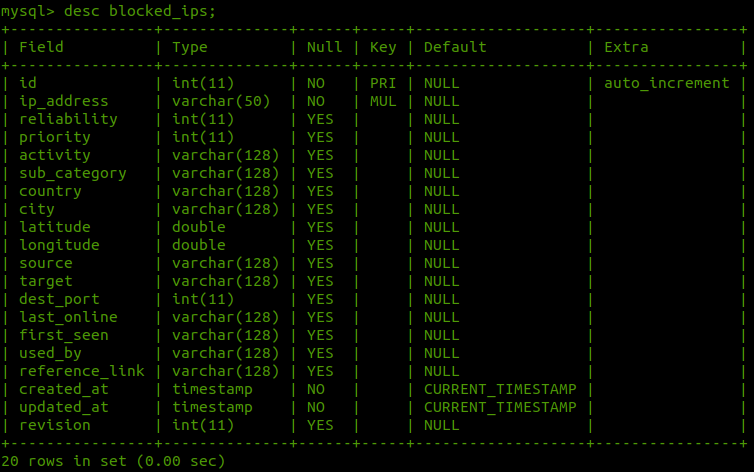
**Deployment Environment Details:**

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

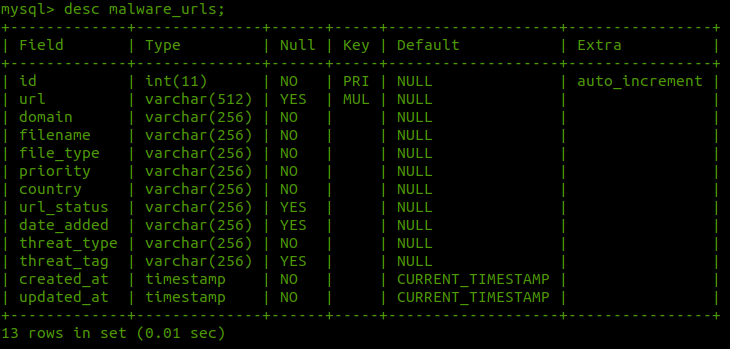
**Database Details:**

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

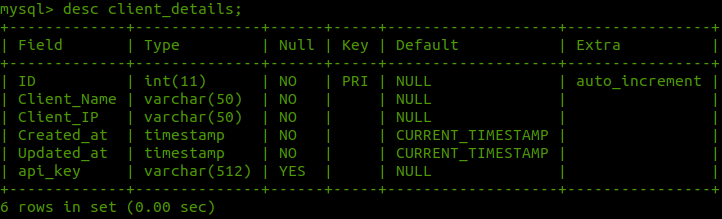
**blocked\_ips table**

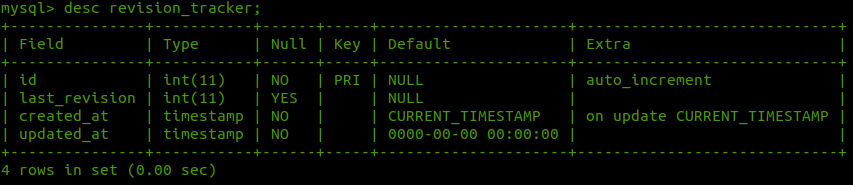


**malware\_urls table**



**client\_details table**

**revision\_tracker table**



**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