Document of Understanding – Requirement

Threat Intelligent hub

Prepared by

Anurag Gundappa

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 of the document:

This document explains the requirements and limitation of Threat Intelligence hub – A python library for building threat database.

Functional Requirement:

The developed threat intelligent hub in written in Python3. It needs following components to work smoothly.

- The set of URLs aka Parsers which is going to fetch data from different threat data sources available on internet.
- The URLs needs to fetch data for reputed IP addressess as well as for malware URLs in specified format. The response of these endpoints must be in JSON with predefined key value structure.
- The table to store data, for IP address, for Malware URLs and to store revision number for IP address.
- A set of python packages which is mentioned in **requirements.txt**

Impact Analysis:

Impacted Area of SIEM is-

Events→Open Threat Exchange

Benefits (Value Add with Change):

- This feature eliminated the need of Open threat exchange database for LTS. Now LTS has its own threat database to show the reputed IP address information.
- The proposed feature also helpful in LTS ecosystem with other components like CASB. Here we are exposing threat database with set of APIs some of them are integrated with CASB plugins.

Condition/Constraint:

1. To access the data store in threat database there are 10 API endpoints to
2. The **client_ip** address and **client_name** must be present in the **client_details** table.
3. To get access token, threat database user must be registered by accessing one of the register API endpoint **threatdb.leosysnet/api/register**
4. This access token must be present in header of every subsequent request under **Authorization key**