Document of Understanding – Requirement

**Threat Intelligent hub**

**DELETION MODULE**

Prepared by

**Anurag Gundappa**

**Background:**

Currently threat intelligence is performing two operation insertion and updation, on the table blocked\_ips, malware\_urls table. This is okay until reputation.data file became unmanageable. There has to be a way to whitelisting the ip\_address present in the table.

Now we are fetching data from [www.BlockList.de](http://www.BlockList.de/) which is a free and voluntary service provided by a Fraud/Abuse-specialist, whose servers are often attacked via SSH-, Mail-Login-, FTP-, Webserver- and other services. The mission is to report any and all attacks to the respective abuse departments of the infected PCs/servers, to ensure that the responsible provider can inform their customer about the infection and disable the attacker. They use the whitelist from [www.dnswl.org](http://www.dnswl.org/), [www.spamhauswhitelist.org](http://www.spamhauswhitelist.com/en/usage.html) and the Blacklist from [torproject.org](http://www.torproject.org/) to reduce false-positive results.

This proposed site itself store reputed IP address details for 48 hours. After the stated period has expired the IP address data is going to be updated.

**Purpose of the document:**

This document explains the requirements and background of Threat Intelligence hub - Deletion module. A python module to integrate with threat intell hub.

**Functional Requirement:**

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

* To delete the IP address data, there has to be a protocol on which this deletion will be based on. Now we are going to clear the **blocked\_ips** table before data insertion will start. In this way we are making sure that only latest IP data will get placed in the database.
* A set of python packages which is mentioned in **requirements.txt**

**Impact Analysis:**

Impacted Area of SIEM is-

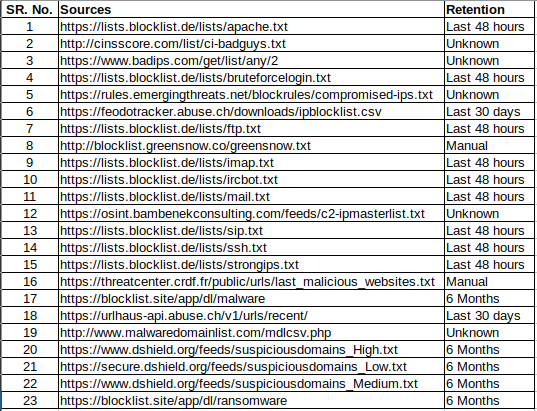
Events→Open Threat Exchange

**Benefits (Value Add with Change):**

* This module eliminates the issues that arises due to heavy data in the tables. Now we have insertion, updation as well as deletion of the data.
* Blocked IP address data will be updated every 48 hours, so there will be old data removal and updated data insertion.
* Our 2 database API [http://threatdb.leosys.net/api/ip/list](http://threatdb.leosys.net/ip/list) and <http://threatdb.leosys.net/api/url/list> which are currently suffering from heavy data response. After implementation of this module this problem will get eliminated and the response time of such endpoints will get reduced.

**Challanges:**

* Currently we are fetching data from the following sources. Every source has its own policy and IP block listing period.
* Variable retention period of keeping the IP address block by each data source providers.
* Some sources whitelist IP address only on manual request from IP address owner.
* Finally there is no proper and predefined criteria which supports IP unblocking/ whitelisting.
* It would be better if we are updating our threat database with new data coming from the source every 48 hours.



**Condition/Constraint:**

1. The main.py which is starting point of threat intelligent hub needs to be run periodically. In our case we are going to run it every 48 hours.
2. This entry point will flush all the data in table which was arrived 48 hours ago . This way only new data will be placed into the table.