**LTS Secure 5.0**

Implementation Document for

**Azure log forwarder**

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 |  |  |  |
| 2.0 | 23-12-2019 |  | New module developed | Purpose, Feature detail, Other details |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Content

**Introduction/Background:**

**Purpose**

**LTS Secure – Feature details**

**Change in Files:**

**User Interface Details :**

**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:**

**Other Details**

**How to run?:**

**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**