Document of Understanding – Requirement

**Azure log forwarder**

Prepared by

**Anurag Gundappa**

**Background:**

As we developed AWS log forwarder to collect logs from AWS platform. Now we want to develop Azure log forwarder for integrating with SIEM. All the events generated by Azure console (Resource logs, Activity logs) needs to be collected by using code and and send them to the sensor in real time over syslog.

**Purpose of the document:**

This document explains the need and understanding of how to collect and build the SIEM plguin for Azure logs

**Functional Requirement:**

Gather all Azure activity logs in real time. Sends them to the Sensor over syslog or write the azure log file located in **var/log/azure.log**

As seen Azure store its all logs in Azure Monitor -> Activity Logs. The proposed architecture suggest that fetching logs from Activity logs is easier.

Azure also has tight binding with python. Azure published Python SDK for Azure and we are leveraging it for this implementation.

Workflow would be like install Azure CLI, Authenticate with Monitor client and fetch activity logs each time scripts run.

Script is responsible for fetching only latest logs which has arrived since last run. This script can be scheduled with scheduler such as crontab.

**Impact Analysis:**

Impacted Area of SIEM is-

Events→Security Events → Datasource → Azure

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

With building out this complete automation LTS SIEM will be able to consume azure logs and monitor complete Azure infrastructure.

**Challanges:**

Currently not having any

**Condition/Constraint:**

1. Azure accounts and associated subscription needs to be setup
2. Setup sensor local deployment -
3. Install Azure CLI
4. Login through Azure login