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**

**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:**

Azure accounts and associated subscription needs to be setup

Setup sensor local deployment -

Install Azure CLI

Login through Azure login