**LTS Secure 5.0**

Implementation Document for

**AWS- Console log generator**

Prepared by

**Anurag Gundappa**

Document Details

|  |  |
| --- | --- |
| Project / Name | LTS Secure - SIEM |
| Current Version | 1.0 |
| List of Contributors |  |
| Customer Contact Information |  |

| Prepared by | Reviewed by | Approved by/Date |
| --- | --- | --- |
| Anurag Gundappa | Nalini Singh |  |

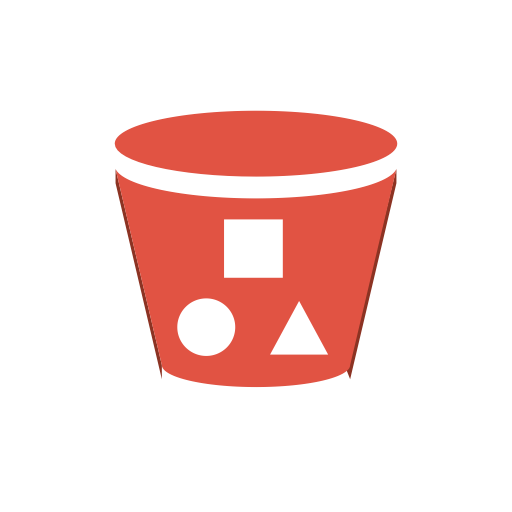
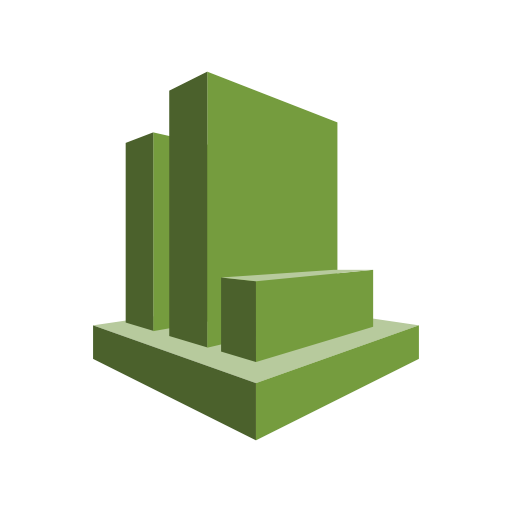
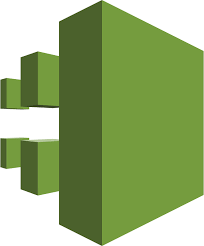
Revision History

| Version | Date | Description of Change | Reason for Change | Affected Sections |
| --- | --- | --- | --- | --- |
| 1.0 | 11-01-2020 | Draft |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Content

**Introduction/Background:**

Amazon Web services is the major cloud service in the market. Various applications, services are hosted by AWS. It is becoming de facto standard for deployment. Monitoring AWS services is essential these days. We are using Python APIs to build our AWS log collector plugin.

****

CloudTrail

S3 Bucket

CloudWatch

AWS

**LTS-AWS INTEGRATION**

**Purpose**

This AWS log collection plugin helps to track and monitor whole AWS cloud services. Currently the service which are able to send the logs to cloudwatch are supported. This AWS-LTS integration is important as far as cloud security is concern. Now the cloud infrastructure can also be monitored with this AWS plugin.

**LTS Secure – Feature details**

This AWS log generator is composed of two plugins

**1. Python app**

This Python app is responsible to collect logs in real time from AWS cloudwatch log group created earlier. This code fetches the logs and sends to the LTS logger over UDP socket. From logger we are sending these logs to LTS SIEM through Logger OUTPUT stream.

This code is basically never ending loop which is fetching AWS logs from CloudWatch service. The script name is “main.py” and it is running in the background with the help of linux screen utility. The status of this script can be obtained by using the command “screen -ls”.

**2. SIEM plugin**

This is normal SIEM plugins installed at ***etc/*ossim/agent/plugins/aws-console.cfg.** This is responsible to generate events from incoming logs to the ***var/*log/alienvault/devices/10.10.10.234/10.10.10.234.log**

Currently there are 69 categories of the AWS events. These categories can be increased. We also supports Generic events generated at AWS.

**Change in Files:**

The new aws-console SIEM plugins needs to be installed.

1. aws-console.cfg needs to be installed at sensor or SIEM at ***etc/*ossim/agent/plugins/.**
2. aws-console.sql needs to be run on SIEM at ***usr/share/doc/mysql-ossim/contrib/plugins/***

**User Interface Details :**

LTS SIEM can show aws-console plugin in

“**Events => Security Events => Datasource => aws-console”**.

All AWS logs can be seen here in real time.

**Deployment Environment Details:**

* **SVN-repo:**
* [http://172.16.0.20/L](http://172.16.0.20/centralised_t_intelligence/threat-intell-hub/)TS-Addons/log-generators/aws-console
* **Deployment location:**
* 172.16.0.188/home/log-collectors/aws-console/

**Database Details:**

There is no need of database in developing this plugin. We are fetching AWS logs at real time and injecting into logger.

**Other Details**

**Project Directory and modules:**

This includes the following directory structure

**log-generators/**

**aws-console/**

config.py

logcollector.py

main.py

setup.cfg

**ibm-bigfix/**

**kaspersky-sc-db/**

**mcafee/**

**splunk/**

**symantec/**

**requirements.txt**

**README.md**