SOW - Centralized logging and analysis of multi-regional AWS WAF logs



**MothersonSumi INfotech & Designs Ltd.**

(A CMMi Level 5 Company)

C-26, Sector-62, NOIDA-201309, India

Website: [www.mind-infotech.com](http://www.mind-infotech.com)

**Bishan Chauhan**

+91 – 120 4365 124

Bishan.Chauhan@mind-infotech.com

The information in this document shall not be duplicated, used, or disclosed in whole or in part outside the customer. If a contract is awarded to MothersonSumi INfotech & Designs Ltd. (MIND) as a result of or in connection with the submission of this document, MIND shall have the right to duplicate, use, or disclose the information within its organization to the extent provided by the contract between the customer and MIND. This restriction does not limit the customer’s right to use information contained in this document if it is obtained from another source without restriction.

Contents

[1. Introduction 3](#_Toc58598916)

[2. Purpose of Centralized logging and analysis of multi-regional AWS WAF logs 3](#_Toc58598917)

[3. Scope of Work 4](#_Toc58598918)

[3.1 Scope 4](#_Toc58598919)

[3.2 Architecture Diagram 5](#_Toc58598921)

[4. Delivery Timelines 5](#_Toc58598922)

[5 Assumptions 6](#_Toc58598923)

[6 Applicable Terms 6](#_Toc58598924)

# Introduction

MothersonSumi INfotech & Designs Ltd. (MIND) is a part of Joint venture between **Samvardhana Motherson Group** (SMG) of India and **Sumitomo Wiring Systems** of Japan (SWS).

MIND is a provider of end-to-end software and engineering design solutions to companies around the globe. MIND started as an IT arm of the group in the year 2000 to support the IT needs of Samvardhana Motherson Group and Sumitomo Wiring Systems worldwide. MIND has further ventured into European and American Market to customers who are non-SWS and SMG to expand our services.

MIND's headquarters and development centers are located in Noida (near New Delhi), India. MIND is a CMMi Level 5, an ISO 9001:2008 and ISO 27001 certified company. Since its inception in 2000, MIND has emerged as a strong world class IT Company with projects across the globe. MIND has multi-lingual software development capabilities including Japanese and German.

MIND is a Microsoft Gold Certified Partner, AWS, Azure & Google Cloud Service Provider, Oracle GOLD OPN partner and also partner with other big IT brands.

MIND has Data Center (Level 3) services, Security Consulting Services Enterprise IT Helpdesk (Multi-lingual), Remote Application Management, Performance Management & Capacity Planning, Network Management Services and Application Hosting. MIND has defined Business Continuity (BC) and Disaster Recovery (DR) plans to mitigate risk of business disruption for its customers.

# Purpose of Centralized logging and analysis of multi-regional AWS WAF logs

**Business Problem**

HostBooks has an online portal, used by accountants and commerce professionals. They use the portal to use services like GST filing and E-way bill payments.

Though they had an on-premise firewall in place, but the customer was facing multiple challenges in analyzing the logs generated by the firewalls deployed at multiple locations. AWS cloud service WAF can consolidate firewall data from multiple regions at one place.

The biggest challenge here is the collection of WAF firewall logs from client website for analysis and then combining these insights to be displayed together in a single dashboard as a one-stop solution.

The next challenge is performing log analysis which is critical for understanding the effectiveness of any solution offered, it is valuable for day-to-day troubleshooting and also for long-term understanding of how the application is performing.

Also, while troubleshooting logs from multiple regions, how to perform root cause analysis for exceptional cases like IP repudiation, BOT Requests, 403 error, Firewall blocking is a difficult task.

# Scope of Work

### 3.1 Scope-

MIND discussed the problem with the customer and after analyzing the business problem, it was determined that Amazon Kinesis Data Firehose would fit the business problem. Solution flow proposed consisted of the following steps.

* With the access to full AWS WAF logs, we currently have the ability to analyze all the logs generated by AWS WAF while it’s protects the web applications. In addition, Amazon Kinesis Data Firehose is used to forward these logs to Amazon Simple Storage Service (Amazon S3) for the purpose of archival, and to Amazon Elasticsearch Service for further analysis which is then represented in Kibana as dashboard.
* This allows us to find out in near-real time that which AWS WAF rules are getting triggered, the reason why are they being triggered, and by which request.
* Long-term analysis is also done by creating a historical view of previous logs.
* The Centralized Logging solution offering enables organizations to collect, analyze, and display Amazon WAF logs in a single dashboard.
* These collected logs provide troubleshooting and root-cause analysis for any kind of exception for say Blacklist IP, IP repudiation, BOT Requests, 403 error, Firewall blocking, IP repudiation limit cross etc.
* The offering contains a suite of infrastructure services that deploy a centralized logging solution.
* It uses Amazon Elasticsearch Service (Amazon ES) and Kibana, an analytics and visualization platform that is integrated with Amazon ES, which together results in a unified view of all the log events.
* Amazon Kinesis Data Firehose streams the data coming from WAF to Amazon Elasticsearch Service and concurrently stores the data to S3.
* Then these errors are visualized in Kibana which will use streamed data to perform real-time root cause analysis for exceptions in a customizable, user-friendly dashboard.

### 3.2 Architecture Diagram

Diagram

Description automatically generated

### 4. Delivery Timelines

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Scope Schedule** | | | | | | |
| **Activity** | **Wk1** | **Wk2** | **Wk3** | **Wk4** | **Wk5** | **Wk6** |
| Working on textract console |  |  |  |  |  |  |
| Building Pre-Processing Lambda |  |  |  |  |  |  |
| Building of Post-Processing Lambda |  |  |  |  |  |  |
| Building of lambda function which saved data to DynamoDB |  |  |  |  |  |  |
| Building of the Front-end |  |  |  |  |  |  |

# Assumptions

* Logs are near real time and without any delay.

6. Non-Functional Requirements

1. No specific workload related DR requirements are specified (unless specifically mentioned)
2. Cloud Watch metrices -i.e. workload operational health can be checked using CloudWatch, not applicable for this workload.
3. MIND ensures that capacity matches but does not exceed what is needed for workload, including by using a demand-based, buffer-based, or time-based approach. This will ensure smallest possible Payload size

MIND solutions are designed to keep bandwidth and message costs down by eliminating unnecessary messaging. MIND Architect takes care for optimized data transfer

# 6 Applicable Terms

1. MIND will deliver work as per SoW defined above, and as part of scope mentioned in support, MIND will manage and operate the workload on mutual agreement.
2. MIND will hand over the workload on acceptance of SoW work, hand off responsibilities include (if support is not applicable as part of support scope)
3. Customer will manage the workload account and will be responsible for maintenance of it including security / permissions of the workload