Document 2: Log Enrichment Summary (Task 1.4)

A. Purpose

The goal is to show that the monitoring system (Wazuh/Elastic Security) can automatically add geographical information to raw data like destination IP addresses. This helps analysts quickly determine whether a connection is going to a trusted or suspicious location during incident triage.

B. Summary

GeoIP enrichment was automatically applied to the network activity log, confirming that the destination IP **8.8.8.8** is located in **Mountain View, California, USA**. This geographical context helps analysts quickly verify that the outbound connection is linked to a trusted public DNS service, improving the accuracy and speed of security analysis.