Log Ingestion

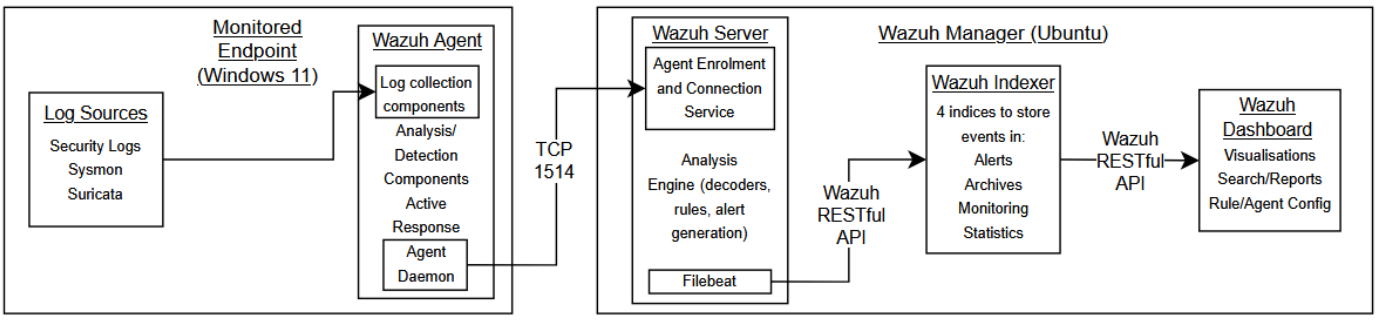

Figure 1: Log Ingestion Pipeline

This SIEM project used a Wazuh-based ingestion pipeline to collect, analyse and visualise security events from Windows endpoints. Logs are collected by the Wazuh Agent, forwarded to the Wazuh server where they are analysed and stored on a centralised indexer for storage and retrieval. The Wazuh Dashboard is the user facing interface that enables viewing, interaction and management with the other components.

1. Log Collection:
   The Wazuh Agent collects logs/events through various sources. Windows event logs are collected through the Log collector module, the FIM (File Integrity module) monitors and reports changes to specified folders in the file system and the command execution module collects the output of authorised commands periodically executed by the agent as some examples.

2. Data Forwarding:
   The Agent forwards this data through the Agent Daemon module via TCP port 1514. The agent Daemon is responsible for managing communication with the Wazuh Server on the Agent side. On the Wazuh Servers side the agent connection service is responsible for collecting this data and forwarding it to the Analysis Engine for processing via decoders and detection rules.

3. Filebeat:
   Alerts generated by the Wazuh Server are then read and forward by Filebeat to the Wazuh Indexer through the Wazuh RESTful API.

4. Data Storage:
   The Wazuh Indexer stores this data under 4 categories of indices as searchable JSON documents.

5. Visualisation and Management:
   The Wazuh Dashboard then queries the indexer to visualise and manage alerts.