Notes

1. **Network Traffic and Data Flow**:

- **Suricata (IDS)**: Suricata is an Intrusion Detection System that monitors and analyzes network traffic for suspicious activities, such as unauthorized access attempts or patterns associated with known attacks. Suricata is configured to inspect network packets, triggering alerts when it detects potentially harmful traffic. These alerts are then sent to Wazuh for further processing and analysis.

2. **Log Collection and Processing**:

- **Beats Agents**: These agents are installed on devices throughout the network to gather logs and other relevant data (e.g., system metrics, file integrity logs). They forward this data to the central processing point.
- **Logstash**: Processes and filters data from Beats and Suricata. It enriches the information before sending it to Elasticsearch, ensuring that data is structured and ready for analysis.

3. **Data Storage and Visualization**:

- **Elasticsearch**: Stores and indexes all the processed data. Elasticsearch makes it possible to search, sort, and analyze the logs from Suricata and other sources.
- **Kibana**: Visualizes the data stored in Elasticsearch through dashboards and graphs, allowing security analysts to quickly identify patterns, trends, and potential security threats in real time.

4. **How Suricata Integrates with Wazuh and ELK (SIEM)**:

- **Suricata** detects threats in real time, such as scans, brute-force attempts, and unusual traffic patterns.
- **Wazuh** receives Suricata's alerts, correlates them with data from other sources, and analyzes patterns to identify potential threats.
- **ELK Stack (Elasticsearch, Logstash, Kibana)** enables centralized storage, analysis, and visualization of Suricata alerts and other logs, giving analysts a comprehensive view of network security.

This setup provides a continuous monitoring system where Suricata acts as the "eyes" on network traffic, while Wazuh and ELK transform the raw alerts and data into actionable insights, enabling quick response to emerging threats.