This project focuses on building a practical log analysis system to improve server security. By collecting and analyzing server logs, we aim to automatically detect suspicious activities like brute force attacks and unauthorized access.

**Setup:**

We will create an experimental environment focused on server log analysis. Our setup will simulate a system administration scenario using log datasets and tools like Kibana and Grafana for visualization. The analysis environment will run on Linux-based systems, as servers typically generate more diverse and detailed security logs. The project will focus on detecting suspicious activities such as repeated failed login attempts, account lockouts, and privilege escalations.

**Data:**

We will use [**Cybersecurity Threat Detection Logs**](https://www.kaggle.com/datasets/aryan208/cybersecurity-threat-detection-logs?utm_source=chatgpt.com)from Kaggle, which contain system and authentication events from various servers. The data will include entries such as login attempts, process creation, and system errors that can indicate potential security incidents or anomalies.

**Expected Outcomes:**

We aim to demonstrate how log analysis and visualization can be used for threat detection in server environments. By applying detection rules and visualizing results with Kibana and Grafana, we expect to identify patterns of suspicious activity and show how such dashboards can help system administrators monitor systems effectively and respond to incidents quickly.