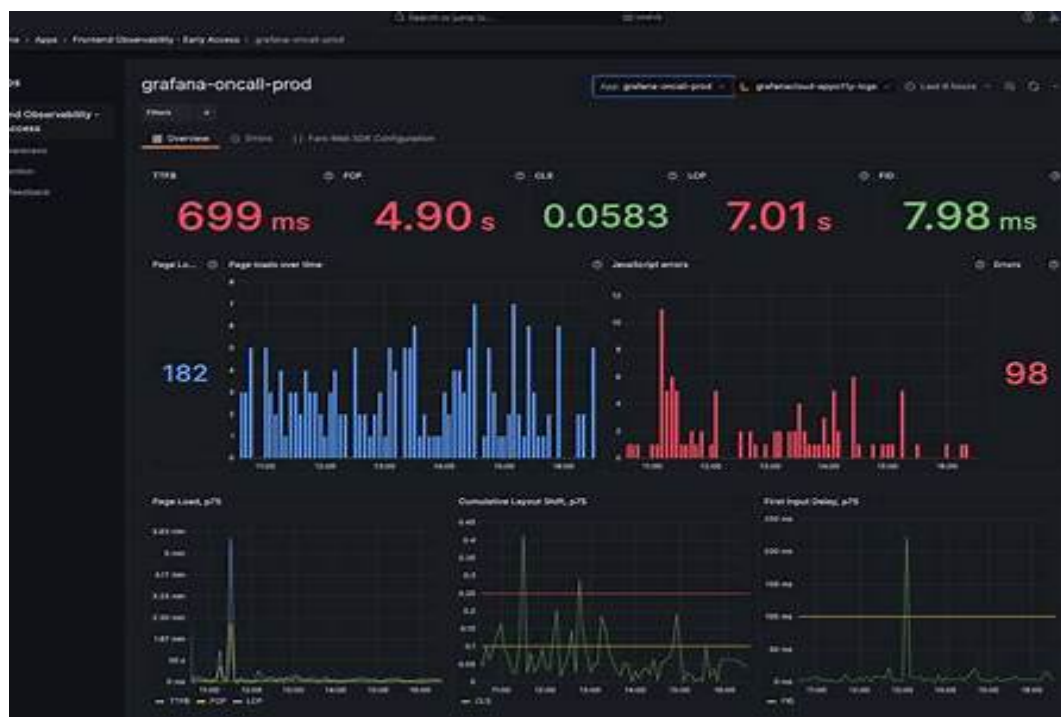
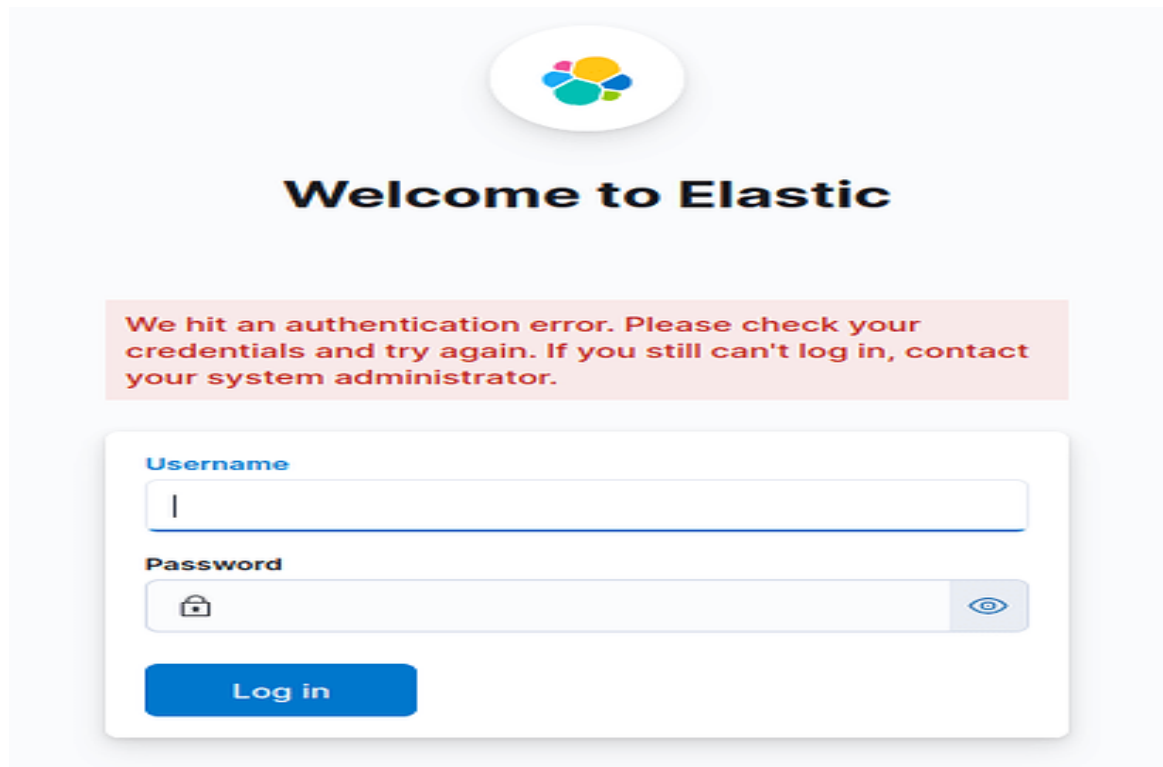


Monitoring Dashboards



Tools Used

- Elastic (Kibana)
- Grafana Labs

Dashboards Created

◆ Visualization 1: Top 10 Source IPs

- Data source: security-*
- Metric: Count of events
- Bucket: Source IP

◆ Visualization 2: Event ID Frequency

- Event IDs:
 - 4625 (Failed login)
 - 7045 (Service creation)

◆ Sigma Rules Used

- Brute-force detection
- Credential abuse rules