

Timeline

| WEEK | TASKS |
|-------------|---|
| Week 1 | Set up Linux/Windows environment and install Kibana & Grafana |
| Week 2 | Preprocess and ingest logs into the visualization tools |
| Week 3 | Create detection rules (failed logins, account lockouts, privilege escalations) |
| Week4 | Design dashboards in Kibana and Grafana |
| Week 5 | Analyze and test detection results |
| Week 6 | Prepare final report and presentation |

Members and Responsibilities

Saanvi Shah:

- Lead data collection and preprocessing from Kaggle.
- Handle data cleaning and formatting for ingestion.
- Build and customize Kibana dashboards.
- Help summarize findings for the final report.

Afla Rafeek:

- Set up Linux and Windows environments.
- Configure log ingestion pipelines (how data moves into Kibana/Grafana).
- Develop detection rules (failed logins, account lockouts, privilege escalation).
- Document setup procedures.

Elijah A. Acero:

- Work on Grafana visualizations and dashboard design.
- Perform data analysis and result interpretation.
- Assist with testing and validation of detection accuracy.

- Lead preparation of the final presentation.