Intern Task Document: Building an OpenSearch–based Security Analytics Platform (HELK Alternative)

Project Title:

O-SIEM: OpenSearch-Based Security Analytics Stack

Objective:

Build a security analytics and threat hunting platform inspired by HELK (Hunting ELK), but using the **latest version of OpenSearch** and related components. The platform should be deployable using **Docker Compose** and serve as a base for **threat hunting, incident response, and log analysis** from various sources including Windows, Linux, firewalls, and cloud services.

Key Deliverables:

1. **Docker Compose Stack**
    - Create a docker-compose.yml to orchestrate all required services:
        - **OpenSearch** (latest version)
        - **OpenSearch Dashboards**
        - **Ingest tools** (e.g., Logstash or OpenSearch ingest pipelines)
        - **Kafka or Beats** (optional for advanced ingestion)
        - **Syslog server** or agent support (e.g., Filebeat, Winlogbeat, Syslog-ng)
        - **Security management plugin** for OpenSearch (configure roles, users, TLS)
        - Any additional services required for scalability, enrichment, or normalization
2. **Initial Configuration Automation**
    - Automatically configure:
        - Dashboards
        - Saved searches / visualizations

        - Example ingest pipelines
        - Index templates
        - Mappings for common log formats (Windows Event Logs, Syslog, JSON logs, etc.)

3. **Testing & Validation**
    - Validate the platform by:
        - Ingesting test logs (e.g., from Windows Event Viewer using Winlogbeat)
        - Creating basic visualizations/dashboards
        - Verifying user authentication and access control
        - Testing log pipelines end-to-end
4. **Documentation**
    - Step-by-step setup guide for:
        - Developers (local use)
        - End users (install, configure, send logs)
        - Security analysts (using dashboards, visualizations, queries)
    - Include:
        - Architecture diagram
        - Troubleshooting guide
        - Sample log files and expected behavior
        - Security hardening tips (basic)

Guidance and Resources:

- **Reference Project:**

  HELK GitHub Repo

  Review how HELK integrates Elastic, Logstash, Kafka, and Beats for threat hunting.
- **OpenSearch Docs:**

    - https://opensearch.org/docs/latest
    - https://github.com/opensearch-project
- **Docker Compose Examples:**
    - https://github.com/opensearch-project/opensearch-dashboards-docker
    - https://github.com/deviantony/docker-elk (for ELK-based inspiration)
- **Log Sources (Suggestions for Testing):**
    - Winlogbeat
    - Filebeat
    - Zeek logs
    - Syslog-ng

Timeline Suggestion (Flexible):

Week	Goals
1	Research HELK & OpenSearch stack components, finalize service list
2	Build and test base Docker Compose setup
3	Add log ingestion support (beats, syslog), test ingest pipelines
4	Configure dashboards, sample queries, saved searches
5	Add security hardening (TLS, roles, auth), polish user experience
6	Document everything; validate deployment from scratch

Success Criteria:

- One-command setup using Docker Compose
- Successful ingestion of at least 3 different log sources
- Working dashboards in OpenSearch Dashboards
- Clear and complete documentation for users and developers

- Intern can demonstrate a threat hunting use case using test logs

---

Bonus Goals :

Note : To be done only when the project is stable and ready for release.

- Integration with Sigma rules (converted to queries)
- Add enrichment with threat intel feeds (MISP, abuse.ch, etc.)
- Export saved objects (dashboards, searches) as a prebuilt .ndjson import
- Publish as an open-source GitHub repo (with CI)