# SOC Analyst Lab Environment

## Overview

This lab creates a small, self-contained environment used to learn basic security monitoring and incident response tasks. It uses a lightweight, local deployment of industry-standard tools so you can build dashboards, review logs, and practice writing incident reports — all on your MacBook, without touching any production systems.

## What’s included

• A local search and analytics engine (Elasticsearch) to store and index log data.

• A web interface (Kibana) that lets you explore logs, build visualizations, and assemble a dashboard.

• Small, optional Python helper scripts that can add example events to the system for practice (kept separate so the core setup remains clean).

## How it was created

1. Installed Docker on the Mac to run services in isolated containers. Docker makes it easy to run Elasticsearch and Kibana together without changing your main system setup.

2. Launched Elasticsearch (single-node) and Kibana in Docker containers and confirmed they can talk to each other. This provides a local place to store, search, and visualize log data.

3. In Kibana, created a data view (index) pointing at the logs so the web interface can read and show events.

4. Built three core visual elements in Kibana: a time-series chart showing authentication outcomes, a pie chart showing which IP addresses are responsible for login attempts, and a log table that behaves like a SOC feed. These visuals are grouped into a single dashboard for quick review.

5. Kept any attack or simulation scripts (for example, brute-force or phishing injectors) in a separate folder so the setup documentation remains strictly about provisioning and verification.

## Why it’s useful

This setup mirrors the real pieces used in many security operations centers: a place to collect logs, tools to search and visualize them, and a dashboard to spot suspicious activity. It’s ideal for practicing detection, triage, and reporting without needing enterprise access.

## Safety & hygiene

The environment is deliberately isolated and local. Attack or simulation scripts are not included in the setup document; run any simulations only in a controlled test environment and never on production networks.