# Macker User's Guide

This project was conducted as part of the education and research project by Team MacneOnTop in the Digital Forensics Track of the Best of the Best (BoB) program, supported by the KITRI(Korea Information Technology Research Institute).

## 1. Project Overview

This project detects anomalous user behavior based on the Apple Unified Logging System (AUL) of macOS.

## 2. Minimum Specifications

For smooth operation, we recommend an environment that meets or exceeds the following specifications.

**HardWare**
**-** CPU: Apple Silicon (M1) or higher recommended
- RAM: 8GB or more

**Disk**
- 20GB or more of free space

**Software**
- macOS Sonoma (14.0) or higher

* Docker Installation Errors
    - Installing Docker via "brew install docker" may cause conflicts with Docker Desktop or errors depending on your environment. We highly recommend using the official Docker Desktop installer.

## 3. Execution Instructions and Basic Information

**Docker Desktop 실행**

```
git clone https://github.com/MACNEONTOP/macker.git
cd macker
chmod +x run.sh
./run.sh
```

* If the login screen displays a white background or fails to load,
  please press Command(⌘) + Left Shift + R.

**Kibana Basic Information**

http://localhost:5601
**ID**: elastic
**PW**: changeme

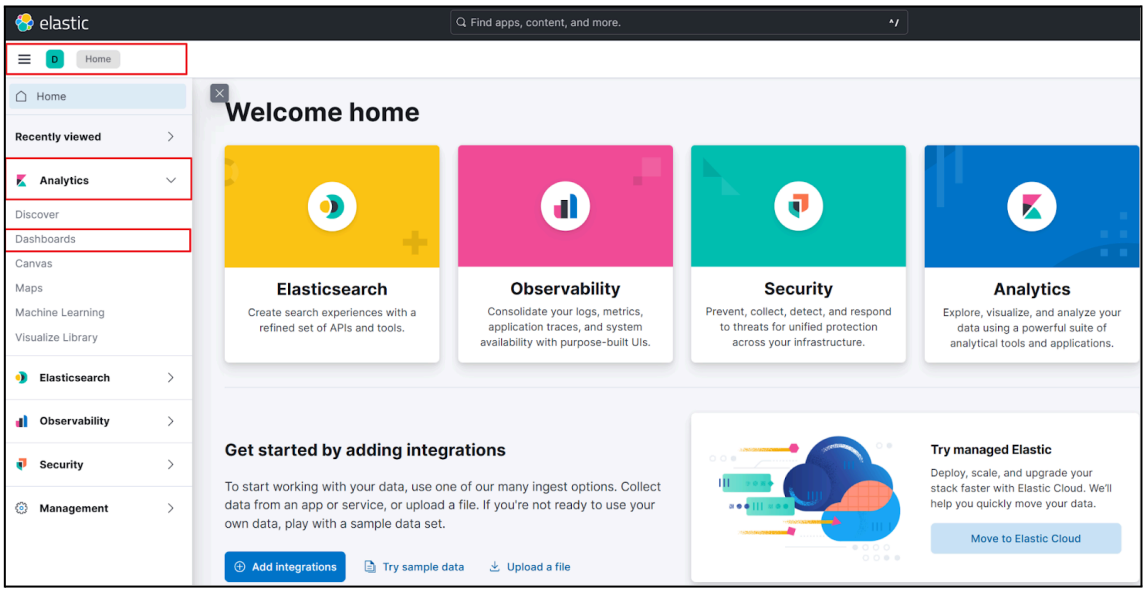
**Deletion and Cleanup**

```
docker compose down -v
```

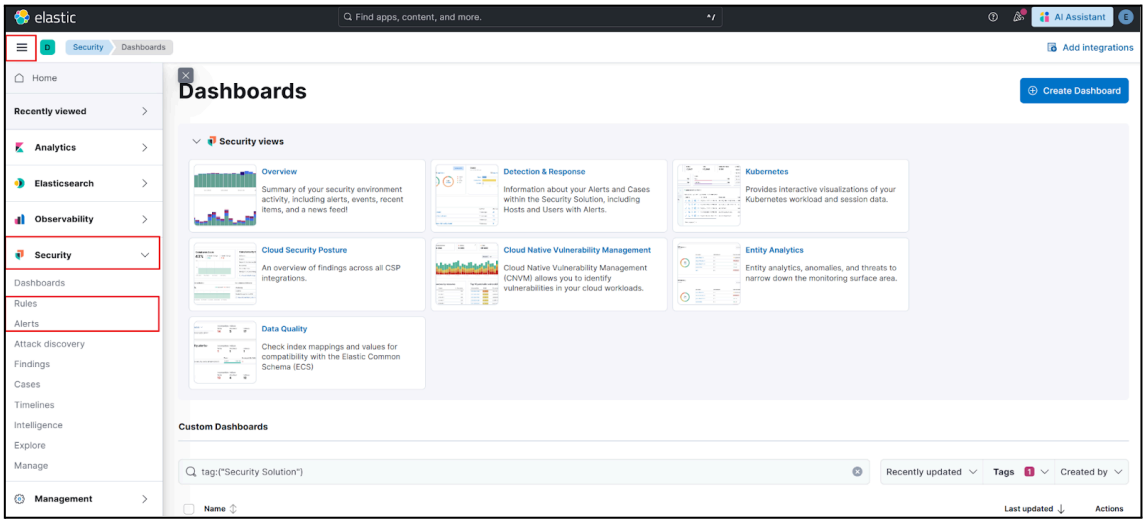
Subsequently, delete the macker folder that you have cloned as git.

# 4. Dashboard

Initial Screen - Navigation Bar - Analytics - Go to Dashboards




## [ Check Detection Rules ]

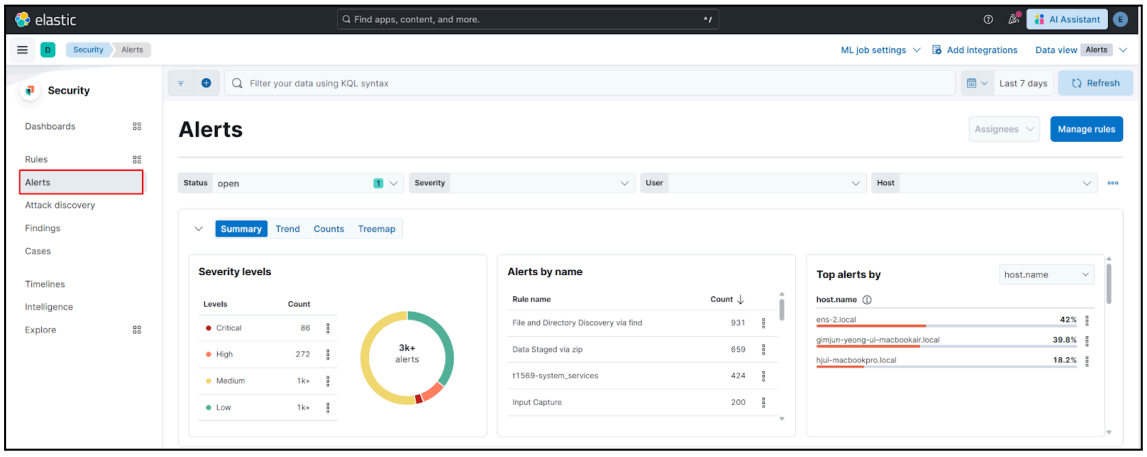



## [ Rules(SIEM) ]

- The Rules page is a space for defining and managing security detection logic, where you can check pre-defined Sigma Rules.

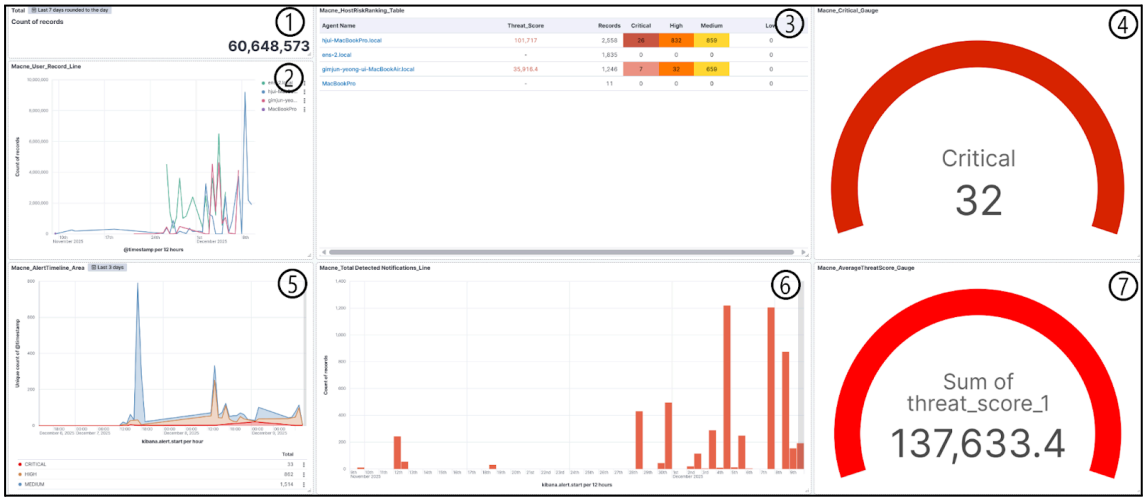
## [ Alerts ]

- This is a space that visually provides events actually detected by active rules.
- When a detection rule finds a log that satisfies the conditions, an Alert is generated, allowing users to immediately identify suspicious activities.




## [ Provided Dashboards ]

## [MacneOnTop] OverView




### ① Count of Records

- You can check logs collected within the last 7 days.

### ② User Record

- You can check the log volume per user and identify abnormal spikes in logs at specific times.

### ③ Host Risk Ranking

- It sorts risk levels in descending order based on Threat Score and detection counts by severity to identify high-risk terminals requiring immediate response.

### ④ Critical Gauge

- You can intuitively check the total count of 'Critical' grade security threat detections requiring immediate action using a gauge chart.

### ⑤ Alert Timeline

- It displays threat detection trends over time as a stacked area chart based on severity, allowing identification of attack timing and intensity.

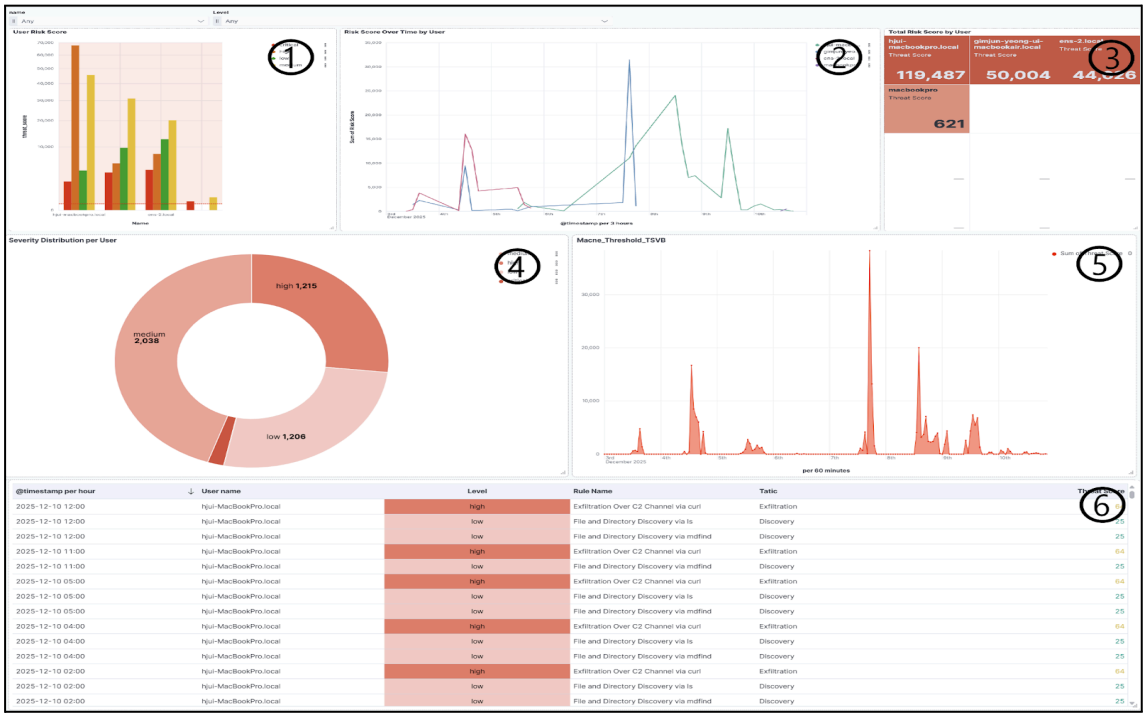
### ⑥ Total Detected Notifications

- It displays the frequency of all security alerts detected during a specific period as a bar graph to check if threat events are concentrated in specific time frames.

### ⑦ Sum of Threat Score

- It represents the total sum of all detected security threat scores; if it exceeds a set threshold, the system's security risk can be determined as critical.

## [MacneOnTop] User-Risk Dashboard




### ① User Risk Score

- You can check the user-level risk score classified into CRITICAL, HIGH, MEDIUM, and LOW grades.

### ② Risk Score Over Time  by User

- You can check the user-level risk score over time.

### ③ Total Risk Score by User

- You can check the total risk score per user.

### ④ Severity Distribution per User

- You can check the count of detected alerts as a pie chart.

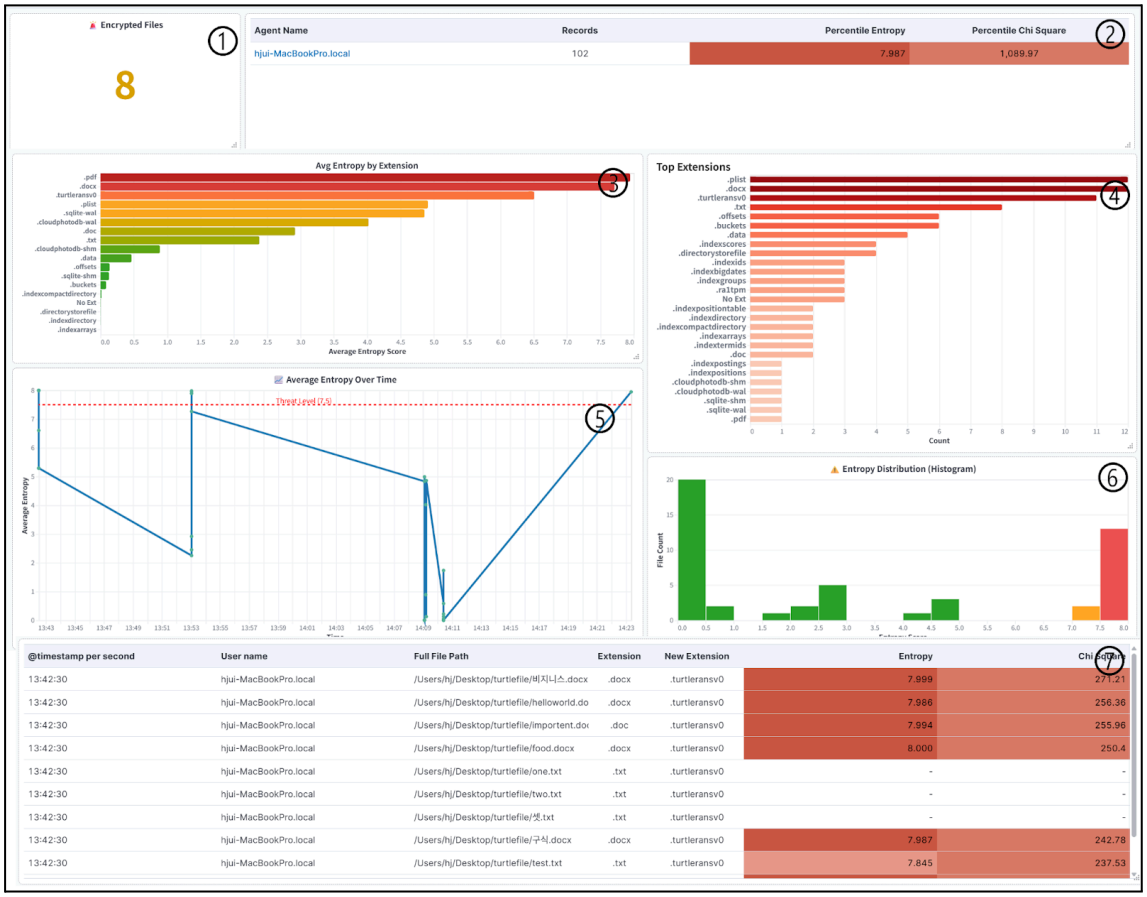
### ⑤ Macne_Threshold_TSVB

- You can check the risk score in 5-minute intervals on a graph.

### ⑥ Detection Rule Details Summary

- You can check detailed information about detected rules, providing items such as occurrence time, username, level, rule name, tactic, and threat score.

## [MacneOnTop] Fsevents Monitoring




## Overview

- This dashboard is specialized for Ransomware detection.
- It is a dashboard that monitors file status changes, primarily allowing monitoring of information related to file encryption.
- It uses calculated entropy values and additional fsevents monitoring, rather than AUL.

- The primary panels for verifying threats are 1, 3, 4, and 7.

### ① Encrypt Files count

- You can check the count of files with a high probability of being encrypted.
- If there is a sudden surge in suspected encrypted files using this panel, ransomware can be suspected.

### ② User Summary

- You can view a summary of the current status of users present in the logs.

### ③ Avg Entropy by Extension

- It calculates and displays the average entropy for each file extension as a graph.
- Suspicious extensions can be identified in this graph.

### ④ Top Extension

- You can check the top 10 extensions with the most recent file events on a graph.
- Suspicious extensions can be identified in this graph.

### ⑤ AVG Entropy Over Time

- You can check the observed entropy over time as a line graph.

### ⑥ Entropy Distribution

- You can check the current distribution status of entropy.

### ⑦ Encrypt Details Summary

- You can check the details of logs where encryption is determined to have occurred.