macker 사용 설명서

본 프로젝트는 과학기술정보통신부가 지원하는 차세대보안리더양성과정(Best of the Best) 디지털포렌식 트랙에서 **막내온탑 팀**이 수행한 교육·연구 과제의 일환으로 진행되었습니다.

1. 프로젝트 개요

본 프로젝트는 macOS의 통합 로깅 시스템(AUL, Apple Unified Logging System)을 기반으로 사용자의 이상행위 탐지합니다.

2. 최소 사양

원활한 구동을 위해 다음 사양 이상의 환경을 권장합니다.

HardWare
- CPU: Apple Silicon (M1) 이상 권장
- RAM: 8GB 이상

Disk
- 20GB 이상의 여유 공간

Software
- macOS Sonoma (14.0) 이상

* Docker 설치 관련 오류
  - brew install docker 방식으로 Docker를 설치할 경우, 환경에 따라 Docker Desktop과 충돌하거나 오류가 발생할 수 있습니다. 가급적 Docker Desktop 공식 설치관리자를 사용 바랍니다.

3. 실행 방법 및 기본 정보

Docker Desktop 실행

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

* 로그인 화면이 흰 배경이 나오거나 로딩이 안되면 Command(⌘) + Left Shift + R 를 사용 바랍니다.

Kibana 기본 정보

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

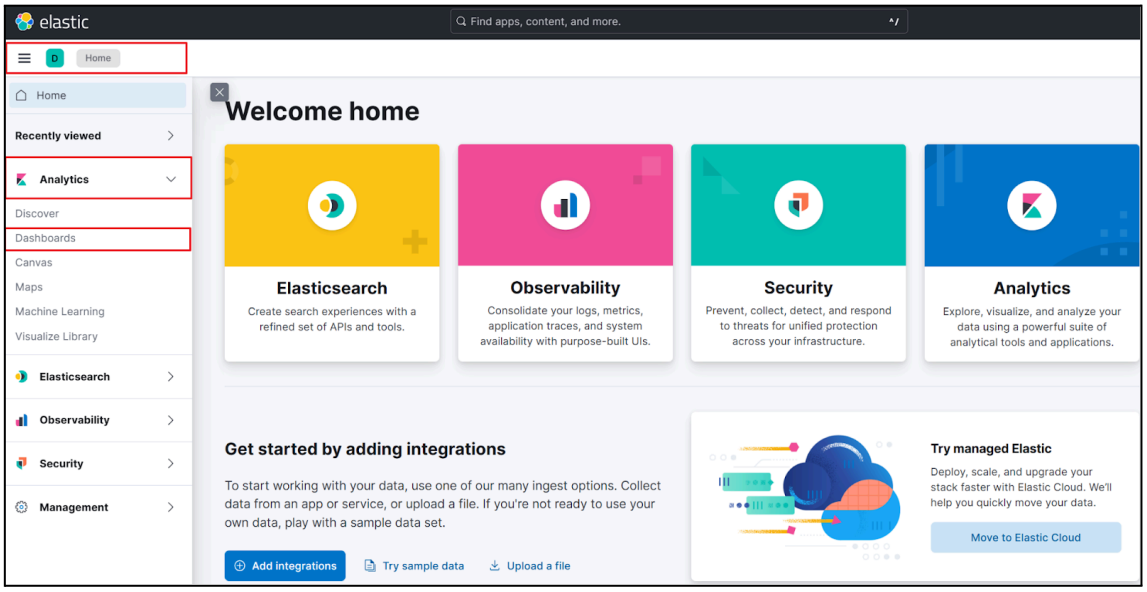
삭제 및 사후 정리

```
docker compose down
```

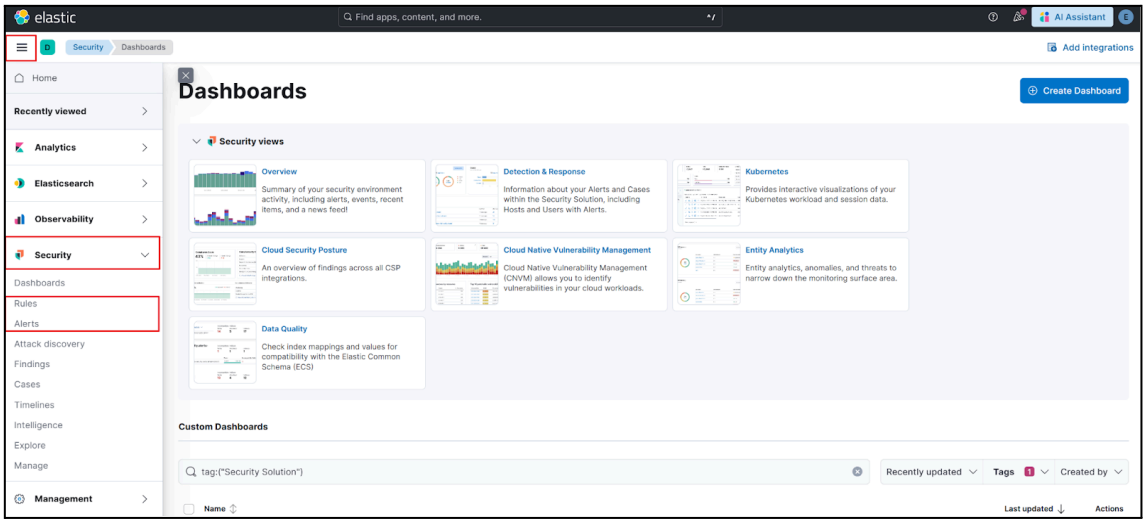
이후 삭제 된 git clone 폴더를 삭제합니다.

4. 대시보드

초기 화면 - 네비게이션 Bar - Analytics - Dashboards 이동



[탐지 룰 확인]

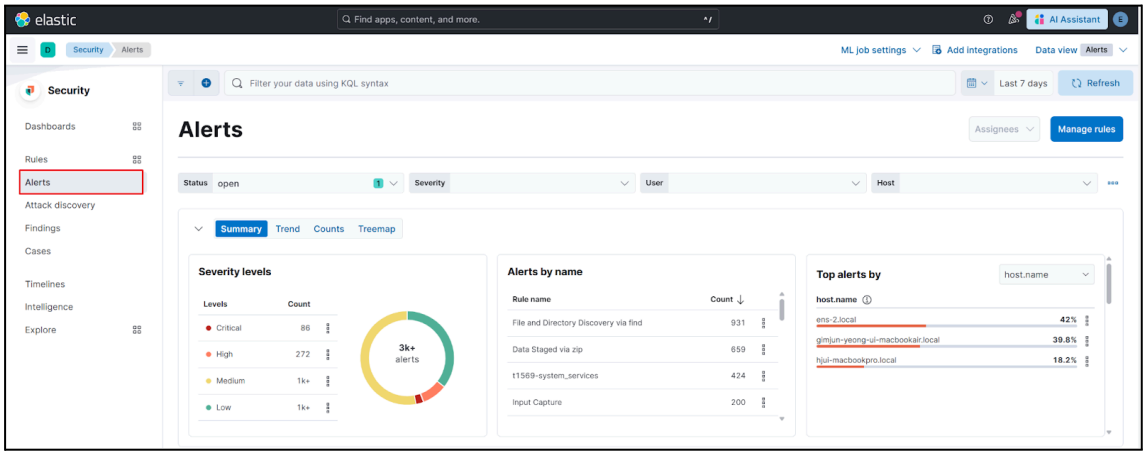


[Rules(SIEM)]

- Rules 페이지는 보안 탐지 로직을 정의하고 관리하는 공간으로 사전에 정의 해둔 Sigma Rules를 확인 가능합니다.

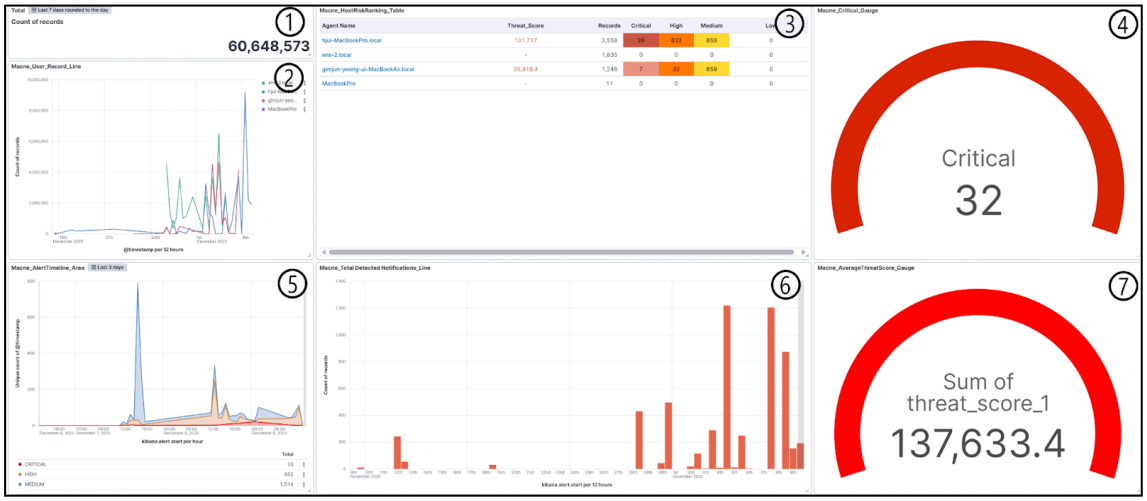
[Alerts]

- 활성화된 규칙들이 실제로 탐지한 이벤트를 시각적으로 제공하는 공간입니다.
- 탐지 규칙이 조건을 만족하는 로그를 발견하면 Alert(경보)이 생성되며, 사용자는 이를 통해 의심스러운 활동을 즉시 확인 가능합니다.



[제공된 대시보드]

[MacneOnTop] OverView



① Count of Records

- 최근 7일 내 수집된 로그를 확인할 수 있습니다.

② User Record

- 사용자 별 로그 발생량을 확인할 수 있으며, 특정 시점의 비정상적인 로그 급증을 식별할 수 있습니다.

③ Host Risk Ranking

- Threat Score와 심각도 별 탐지 건수를 기준으로 위험도를 내림차순 정렬하여, 우선 대응이 필요한 고위험 단말을 선별합니다.

④ Critical Gauge

- 즉각적인 조치가 요구되는 'Critical' 등급의 보안 위협 탐지 총건수를 게이지 차트로 직관적으로 확인할 수 있습니다.

⑤ Alert Timeline

- 시간대별 위협 탐지 추이를 심각도에 따라 누적 영역 차트로 표현하여, 공격 시도의 발생 시점과 집중도를 파악할 수 있습니다.

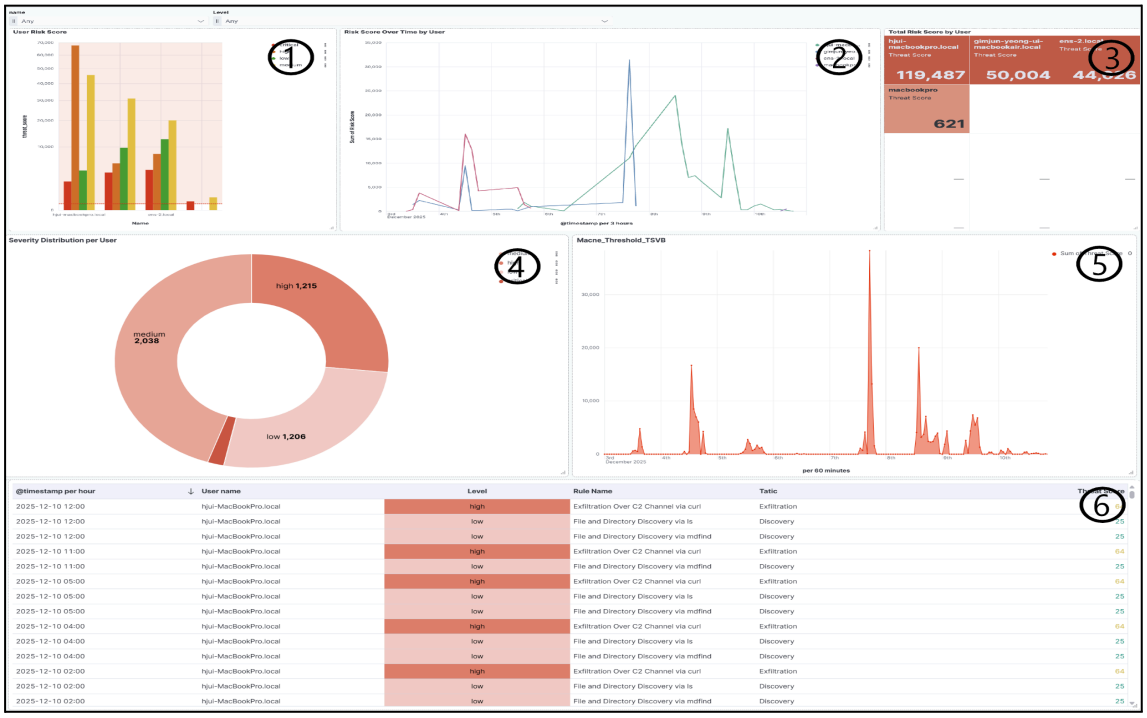
⑥ Total Detected Notifications

- 일정 주기 동안 탐지된 전체 보안 알림의 발생 빈도를 막대그래프로 나타내어, 특정 시간대에 위협 이벤트가 집중되었는지 확인할 수 있습니다.

⑦ Sum of Threat Score

- 탐지된 모든 보안 위협 점수의 총합을 나타내며, 설정된 임계값을 초과할 경우 시스템의 보안 위험도가 심각한 수준임을 판단할 수 있습니다.

[MacneOnTop] User-Risk Dashboard



① User Risk Score

- 사용자 단위 위협 점수를 CRITICAL, HIGH, MEDIUM, LOW 등급으로 구분하여 확인할 수 있습니다.

② Risk Score Over Time by User

- 시간 흐름 기준으로 사용자 단위 위협 점수를 확인할 수 있습니다.

③ Total Risk Score by User

- 사용자 단위의 위협 점수를 확인할 수 있습니다.

④ Severity Distribution per User

- 탐지된 알림 수를 원형 그래프로 확인할 수 있습니다.

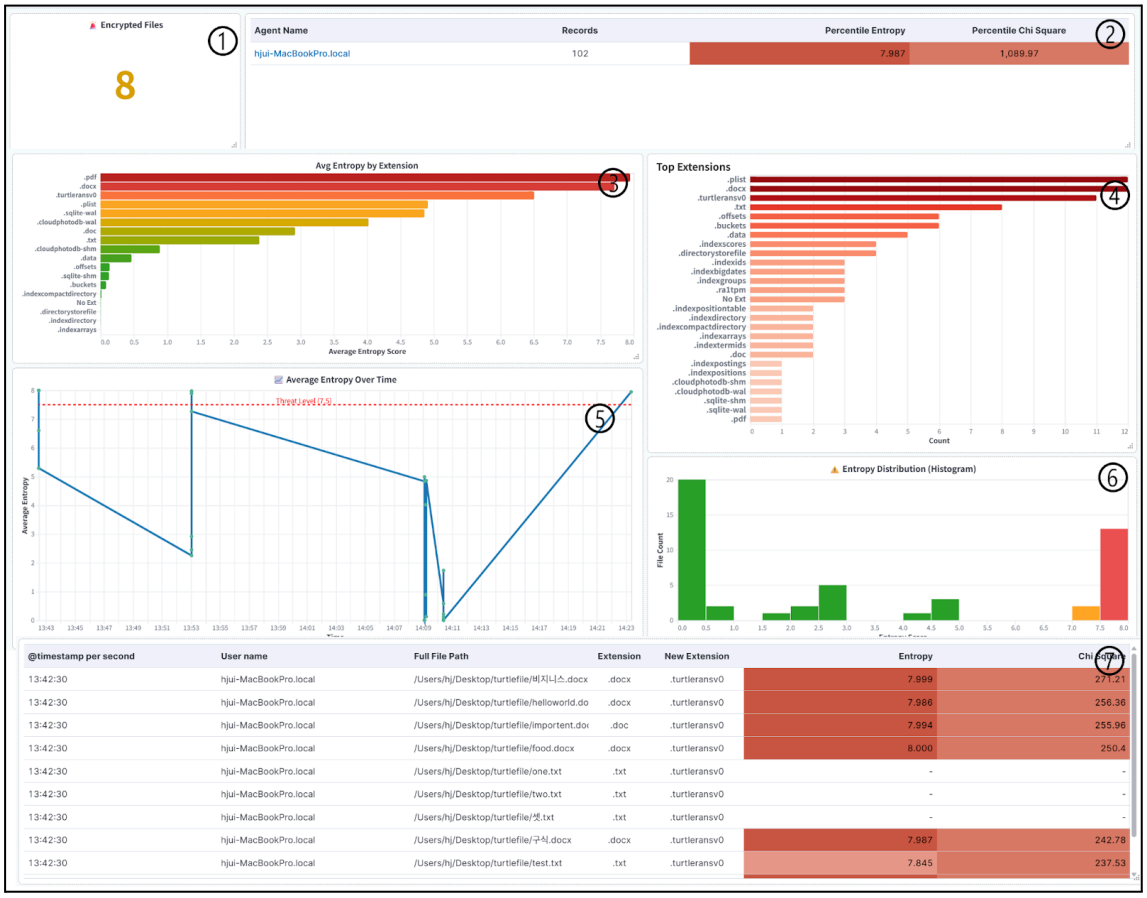
⑤ Macne_Threshold_TSVB

- 5분 단위로 위협 점수를 그래프로 확인할 수 있습니다.

⑥ Detection Rule Details Summary

- 탐지된 룰의 세부 정보를 확인할 수 있으며, 시간대별 발생 시각, 사용자명, 레벨, 룰 이름, 전술(Tactic), 위협 점수 항목을 함께 제공합니다.

[MacneOnTop] Fsevents Monitoring



개요

- 본 대시보드는 Ransomware 탐지에 특화된 대시보드입니다.
- 파일의 상태 변화를 감시할 수 있는 대시보드로, 주로 파일 암호화와 관련된 정보를 모니터링 할 수 있습니다.
- AUL이 아닌 추가 fsevents모니터링과 엔트로피를 계산하여 그 값을 사용합니다.
- 위협성을 주로 확인할 수 있는 패널은, 1번과 3,4번, 7번입니다.

① Encrypt Files count

- 암호화 되었을 가능성이 높은 파일들의 개수를 확인할 수 있습니다.
- 본 패널을 활용하여 갑자기 암호화 의심 파일이 급증하게 되면 랜섬웨어로 의심할 수 있습니다.

② User Summary

- 로그에 존재하는 유저의 현재 상태를 요약해서 확인할 수 있습니다.

③ Avg Entropy by Extension

- 각 확장자 별 평균 엔트로피를 계산하여 그래프로 보여줍니다.
- 수상한 확장자가 해당 그래프에서 확인될 수 있습니다.

④ Top Extension

- 최근 파일 이벤트가 가장 많이 발생한 10개의 확장자를 그래프로 확인할 수 있습니다.
- 수상한 확장자가 해당 그래프에서 확인될 수 있습니다.

⑤ AVG Entropy Over Time

- 시간 순서로, 관측된 엔트로피를 꺾은선 그래프로 확인할 수 있습니다.

⑥ Entropy Distribution

- 현재 엔트로피의 분포 현황을 확인할 수 있습니다.

⑦ Encrypt Details Summary

- 암호화가 일어났다고 판단되는 로그에 대해 세부적으로 확인할 수 있습니다.