

대시보드 · 관제

패널 조립 · 시간범위 · Auto refresh · 전역 KQL 필터

01

대시보드 조립

저장한 시각화를 패널로 모아 한 화면 구성

02

시간·갱신

시간범위와 Auto refresh로 실시간 관제

03

전역 필터

대시보드 KQL로 전 패널 동시 필터링

04

SOC 관제

보안 관제 화면 구성과 운영 팁

S5

대시보드 관제

세션 개요와 학습 목표

저장한 시각화를 패널로 조립해 실시간 SOC 관제 화면을 만든다.

이 세션에서 얻는 것

- **패널 조립**: 앞 세션에서 저장한 시각화들을 Dashboard에 추가해 한 화면으로 모으는 절차를 익힌다.
- **실시간 관제**: 시간범위와 Auto refresh를 설정해 데이터가 주기적으로 갱신되는 관제 화면을 구성한다.
- **전역 필터**: 대시보드 상단 KQL 하나로 모든 패널을 동시에 필터링해 관점을 즉시 전환한다.

대시보드의 역할

- **단일 화면**: 흩어진 지표를 한 화면에 모아 상황을 한눈에 파악하는 관제 캔버스 역할을 한다.
- **실습 연결**: 개별 시각화가 조립돼 SOC 보안 관제 대시보드로 완성되는 과정을 손으로 확인한다.

● 대시보드

○ 패널

○ 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드·관제

대시보드란 무엇인가

여러 시각화를 한 화면에 모은 관제 캔버스가 대시보드다.

개념과 목적

- **관제 캔버스**: 공격 건수·상태코드·트래픽 등 여러 시각화를 한 화면에 배치한 종합 관제 판이다.
- **단일 사실원천**: single pane of glass, 흩어진 지표를 한 곳에서 봐야 상황 판단이 빠르고 정확해진다.
- **역할별 구성**: 경영용 요약, 운영용 상세, 조사용 드릴다운처럼 목적에 맞춰 별도 대시보드를 만든다.

좋은 대시보드의 조건

- **핵심 지표**: 봐야 할 소수의 지표만 담아 노이즈를 줄이고 이상 징후에 시선이 가게 한다.
- **한눈에**: 스크롤 없이 한 화면에서 전체 상황이 읽히도록 중요도 순으로 배치한다.

● 대시보드

○ 패널

○ 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드 관제

패널 추가와 배치

저장된 시각화를 패널로 올리고 드래그로 자리를 잡는다.

추가 절차

- **Dashboard 열기**: 좌측 메뉴에서 Dashboard로 이동해 Create로 새 대시보드를 시작한다.
- **Add로 추가**: 상단 Add를 눌러 앞서 저장한 시각화 목록에서 원하는 패널을 골라 화면에 얹는다.
- **크기·위치**: 패널 모서리를 드래그해 크기를 조절하고 위치를 옮겨 원하는 레이아웃을 만든다.

레이아웃 원칙

- **중요도 순**: 총 공격 건수 같은 핵심 지표를 상단에, 세부 표·분포는 하단에 배치한다.
- **F자 시선**: 사람의 시선이 좌상단에서 시작하므로 가장 중요한 패널을 그 자리에 놓는다.

○ 대시보드

● **패널**

○ 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드 관제

저장과 이름 규칙

공용 환경이므로 이름에 이니셜을 붙여 충돌을 막는다.

저장 방법

- **Save 버튼**: 배치를 마치면 우상단 Save로 대시보드를 저장하고 언제든지 목록에서 다시 연다.
- **복제 후 편집**: 기존 예시를 열어 Save as로 복제한 뒤 편집하면 원본을 보존하며 실습할 수 있다.
- **구성 저장**: 저장 시 패널 배치와 적용된 시간·필터 설정이 함께 보존된다.

명명 규칙

- **이니셜 접두**: 공용 환경이라 이름 앞에 본인 이니셜을 붙인다(예 kim-보안관제).
- **용도 구분**: 버전·용도를 이름에 담아 다른 수강생 산출물과 헷갈리지 않게 한다.

○ 대시보드

● **패널**

○ 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드·관제

시간 범위 설정

우상단 시간 피커가 대시보드 전체 패널에 동시 적용된다.

시간 피커

- **Quick select:** Last 15m·1h·24h 같은 상대 범위를 클릭 한 번으로 지정한다.
- **절대 범위:** 사고 조사 시 시작·종료 시각을 절대값으로 지정해 특정 구간만 본다.
- **전체 적용:** 여기서 고른 범위가 대시보드의 모든 패널에 한꺼번에 반영된다.

활용

- **범위 좁히기:** 이상 징후를 발견하면 시점을 좁혀 스파이크가 발생한 구간을 정밀하게 확인한다.
- **추이 비교:** 넓은 범위로 평상시 흐름을 보고 좁은 범위로 사건 구간을 대조한다.

○ 대시보드

○ 패널

● 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드·관제

Auto refresh 실시간 관제

자동 갱신을 켜면 패널이 주기적으로 새 데이터를 반영한다.

자동 갱신

- **주기 설정:** Auto refresh를 5s·10s 등으로 켜면 패널이 그 주기마다 최신 로그로 다시 그려진다.
- **실시간성:** 새로고침 없이 화면이 스스로 갱신돼 실시간 관제 상황판으로 동작한다.
- **상시 표출:** 대형 모니터에 띄워 두면 상황실에서 계속 흐르는 로그를 관제할 수 있다.

관제 운영

- **주기·부하 균형:** 주기가 짧을수록 신선하지만 서버 부하가 커지므로 적정 간격을 잡는다.
- **조사 시 정지:** 특정 구간을 조사할 때는 자동 갱신을 잠시 꺼 화면이 바뀌지 않게 한다.

○ 대시보드

○ 패널

● 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드 관제

UTC와 시간대 주의

로그는 UTC로 저장돼 표시 시간대와 차이가 날 수 있다.

시간대 이슈

- **UTC 저장:** 모든 이벤트의 @timestamp는 UTC 기준으로 저장되어 있다.
- **표시 차이:** 브라우저는 로컬 시간대로 보여줘 저장값과 화면 표시 시각이 어긋나 보일 수 있다.
- **데이터 없음:** 패널이 비어 보이면 시간 범위를 넓혀 Refresh해 데이터 존재를 먼저 확인한다.

실무 대응

- **UTC 기준 확인:** 사고 시각을 논할 때는 어느 시간대 기준인지 명시해 혼선을 막는다.
- **교차 검증:** 원본 로그의 UTC 값과 화면 표시 시각을 함께 대조해 실제 발생 시각을 확정한다.

○ 대시보드

○ 패널

● 시간·갱신

○ 필터·관제

○ 정리

S5

대시보드 관제

대시보드 레벨 KQL 필터

상단 검색창의 KQL 하나가 모든 패널에 동시 적용된다.

전역 필터

- **동시 필터링**: 대시보드 상단 검색창에 KQL을 넣으면 모든 패널이 같은 조건으로 걸러진다(예 event: attack).
- **필터 pill**: Add filter로 필드·값 조건을 pill 형태로 추가해 KQL과 함께 조합할 수 있다.
- **저장 포함**: 대시보드를 저장하면 적용된 검색어와 필터도 함께 보존된다.

활용

- **공격만 보기**: event: attack으로 좁히면 전 패널이 공격 관점으로 전환돼 관제가 명확해진다.
- **특정 IP**: client_ip 조건을 걸어 한 출발지의 활동을 전 패널에서 드릴다운한다.

○ 대시보드

○ 패널

○ 시간·갱신

● 필터·관제

○ 정리

S5

대시보드·관제

패널 동시 필터 예시

대시보드 검색창 KQL 하나로 전 패널의 관점을 바꾼다.

```
# 공격 이벤트만 - 전 패널 공격 관점
event: attack

# 러시아발 트래픽만 집중 관제
geo.country: RU

# 특정 IP 드릴다운(출발지 조사)
client_ip: "203.0.113.7"

# 서버 오류만 - 장애·DoS 신호
http.status >= 500

# 심각도 높은 공격만
severity: (high or critical)

# 조합 - 러시아발 SQLi 공격
geo.country: RU and attack_type: sqli
```

동시 필터의 힘

- **관점 전환:** KQL 한 줄로 전체 패널이 같은 조건으로 재계산돼 관점이 즉시 바뀐다.
- **드릴다운:** 특정 IP·국가로 좁히면 그 대상의 활동만 전 패널에서 조사할 수 있다.
- **노이즈 제거:** 필터를 조합해 정상 트래픽을 걸어내면 공격 신호만 또렷하게 남는다.

○ 대시보드

○ 패널

○ 시간·갱신

● 필터·관제

○ 정리

S5

SOC 관제 화면 구성

대시보드·관제

SOC 보안 관제 대시보드는 6개 패널로 상황을 한눈에 보여준다.

패널	컴포넌트	관제 포인트
공격 건수	Metric	총 공격 수 급증 여부를 한눈에 파악
상태코드 분포	Donut	4xx/5xx 비율로 오류·공격 신호 감지
공격 유형	Bar	최다 공격 벡터(sqli·xss 등) 식별
국가별 접속	Region Map	서비스 대상 밖 이상 지역 발견
트래픽 추이	Line	시간대별 스파이크·비정상 급증 포착
상위 공격자 IP	Data Table	집중 공격 출발지 IP 특정

○ 대시보드

○ 패널

○ 시간·갱신

● 필터·관제

○ 정리

S5

대시보드·관제

관제 운영 팁

평상시 기준을 알아야 이상을 빠르게 감지할 수 있다.

효과적 관제

- **baseline 파악**: 정상 트래픽의 평상시 수준을 먼저 익혀야 이상 급증을 빠르게 알아챈다.
- **우선순위 표시**: 색상과 임계선을 활용해 위험 수준이 시각적으로 먼저 눈에 띄게 한다.
- **드릴다운 동선**: 지표에서 원인 조사로 이어지는 필터·화면 이동 경로를 미리 설계한다.

흔한 실수

- **패널 과다**: 너무 많은 패널을 얹으면 정작 중요한 신호가 묻혀 판단이 느려진다.
- **인수인계**: 교대 시 무엇을 봐야 하는지 기준이 없으면 이상 징후를 놓치기 쉽다.

○ 대시보드

○ 패널

○ 시간·갱신

● 필터·관제

○ 정리

S5

대시보드·관계

공유·권한과 주의점

공용 환경에서는 원본을 지키며 복제본으로 편집한다.

공유 방법

- **공유 링크**: Share로 대시보드 링크나 임베드 코드를 생성해 관계자와 화면을 공유한다.
- **읽기 전용**: 조회만 필요한 사용자에게는 읽기 전용 역할을 부여해 실수 편집을 막는다.
- **접근통제**: 민감 지표가 담긴 대시보드는 접근 권한을 제한해 열람 범위를 통제한다.

운영 주의

- **원본 보존**: 공용 환경의 공유 대시보드는 직접 수정하지 말고 복제 후 편집한다.
- **이름 관리**: 이니셜을 붙여 저장해 다른 사용자 산출물과 뒤섞이지 않게 한다.

○ 대시보드

○ 패널

○ 시간·갱신

● 필터·관계

○ 정리

S5

대시보드·관제

세션 정리와 다음 예고

패널 조립부터 실시간 관제까지 대시보드 흐름을 정리한다.

기억할 것

- **패널 조립**: 저장한 시각화를 Dashboard에 Add해 중요도 순으로 배치하면 관제 화면이 완성된다.
- **시간·갱신**: 시간범위와 Auto refresh를 설정해 실시간으로 갱신되는 관제 상황판을 만든다.
- **전역 KQL**: 상단 검색창의 KQL 한 줄로 전 패널을 동시에 필터링해 관점을 즉시 전환한다.

다음 예고 — 세션 6

- **위협 탐지**: 브루트포스·스캐너·데이터 유출 등 실제 위협 탐지 시나리오를 다룬다.
- **가설 검증**: 가설을 세워 쿼리로 확인하고 해석·대응까지 잇는 조사 흐름을 실습한다.

○ 대시보드

○ 패널

○ 시간·갱신

○ 필터·관제

● 정리