세션 7

탐지 규칙 · 알럿 · 운영

저장 검색 · Alerting 임계치 규칙 · 오탐 튜닝 · 운영 체크리스트

01
저장 검색
반복 탐지 쿼리를 저장해 재사용·자동화의 입력으로

02
Alerting
Monitor·Trigger·Action으로 상시 감시·통보

03
임계치 규칙
브루트포스·공격 급증을 DSL 임계치로 탐지

04
튜닝·운영
오탐 튜닝·알럿 피로 관리와 운영 체크리스트

S7

탐지 규칙·알럿·운영

세션 개요와 학습 목표

> 반복 탐지 쿼리를 저장 검색과 임계치 규칙으로 자동화하고 운영까지 잇는다.

이 세션에서 얻는 것

- **저장 검색**: Discover에서 만든 탐지 쿼리를 저장 검색으로 만들어 재사용하고 알럿의 입력으로 삼는다.
- **임계치 규칙**: Alerting Monitor로 브루트포스·공격 급증을 5분·10분 창의 임계치로 자동 탐지한다.
- **튜닝과 운영**: 오탐을 줄이는 튜닝 기법과 규칙·인덱스를 지속 점검하는 운영 체크리스트를 익힌다.

수동 탐지에서 자동 탐지로

- **한계 인식**: 사람이 매번 Discover를 열어 검색하는 방식은 놓치는 시간대가 생겨 상시 감시가 불가능하다.
- **자동화 목표**: 저장 검색을 규칙으로 승격해 조건 충족 시 자동 통보되도록 탐지 커버리지를 넓힌다.

● 저장검색
○ 알럿
○ 임계치
○ 튜닝
○ 운영

S7

탐지 규칙·알럿·운영

저장 검색(Saved Search)

> Discover의 쿼리·컬럼·정렬을 하나로 저장해 언제든 같은 뷰를 재현한다.

저장 검색이란

- **구성 저장**: KQL 쿼리와 선택한 컬럼, 정렬, 인덱스 패턴을 묶어 이름을 붙여 저장한다.
- **재현성**: event:auth_fail 같은 탐지 뷰를 매번 다시 짜지 않고 한 번의 클릭으로 동일하게 연다.
- **일관성**: 팀원이 같은 필드·필터로 보므로 분석 기준이 사람마다 달라지는 문제를 줄인다.

활용 — 재현·공유·규칙

- **대시보드 입력**: 저장 검색을 Dashboard 패널로 얹어 원본 로그 테이블을 관제 화면에 포함한다.
- **알럿 기반**: 저장한 탐지 쿼리를 Alerting Monitor의 질의로 재사용해 자동 탐지 규칙으로 승격한다.

● 저장검색
○ 알럿
○ 임계치
○ 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

수동 탐지에서 자동 탐지로

> 사람의 검색은 놓치는 시간을 남기지만, 규칙은 24시간 쉬지 않는다.

자동화의 이유

- **상시성**: 공격은 새벽·주말을 가리지 않으므로 사람이 지켜보지 못하는 시간대의 공백을 메워야 한다.
- **반복 비용**: 같은 탐지 쿼리를 매일 수동 실행하는 것은 비효율적이고 실행을 잊으면 탐지가 누락된다.
- **일관 판정**: 규칙은 정해진 임계치로 판정하므로 담당자 컨디션에 따라 결과가 흔들리지 않는다.

자동화 흐름 — 검색·모니터·통보

- **검색 정의**: 탐지하려는 조건을 저장 검색으로 확정하고 필드·범위를 명확히 한다.
- **모니터·통보**: Monitor가 주기적으로 쿼리를 실행하고 조건 충족 시 채널로 자동 통보한다.

● 저장검색
○ 알럿
○ 임계치
○ 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

Alerting 개념과 Monitor 구조

> Alerting은 Monitor·Trigger·Action 세 구성으로 탐지와 통보를 자동화한다.

구성요소 — Monitor·Trigger·Action

- **Monitor**: 지정한 인덱스에 대해 정해진 주기로 쿼리를 실행해 결과(집계값)를 수집하는 단위다.
- **Trigger**: Monitor 결과를 조건식으로 판정해 알럿을 발생시킬지 결정하는 규칙이다.
- **Action**: Trigger가 참일 때 메시지를 만들어 Slack·이메일 등 채널로 통보하는 실행부다.

실행 주기 — schedule

- **주기 실행**: Monitor는 1분·5분 같은 schedule로 반복 실행되어 최근 로그를 지속 평가한다.
- **관측 창 정합**: 쿼리의 시간 범위(now-5m)와 실행 주기를 맞춰 중복·누락 없이 평가되게 한다.

○ 저장검색
● 알럿
○ 임계치
○ 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

알럿 구성요소 — 트리거·액션·채널

> 트리거는 집계값을 비교하고 액션은 메시지를 만들어 채널로 내보낸다.

트리거·액션

- **조건식**: ctx.results의 집계값(예 client_ip별 실패 수)을 임계치와 비교해 참·거짓을 판정한다.
- **메시지 템플릿**: 액션은 규칙명·심각도·해당 IP·건수를 템플릿에 채워 사람이 읽을 알럿 본문을 만든다.
- **심각도 라벨**: high·critical 같은 라벨을 붙여 수신 측이 우선순위를 즉시 판단하게 한다.

통보 채널·에스컬레이션

- **채널 선택**: Slack·이메일·웹훅으로 보내며 심각도에 따라 서로 다른 채널로 라우팅한다.
- **에스컬레이션**: 미확인 알럿은 상위 담당·온콜로 단계적으로 넘겨 방치되지 않게 한다.

○ 저장검색
● 알럿
○ 임계치
○ 튜닝
○ 운영

S7

탐지 규칙·알럿·운영

브루트포스 임계치 규칙(DSL)

> 5분 창에서 한 IP의 auth_fail이 20회 이상이면 알럿을 발생시킨다.

```
// 목표: 최근 5분간 한 client_ip 의 auth_fail 20회 이상 탐지
// Monitor 실행 주기: 1분 (per query monitor)
{
  "query": {
    "bool": {
      "filter": [
        { "term":  { "event": "auth_fail" } },
        { "range": { "@timestamp": { "gte": "now-5m" } } }
      ]
    }
  },
  "aggregations": {
    "by_client_ip": {
      "terms": { "field": "client_ip", "size": 20 }
    }
  }
}
// Trigger 조건: by_client_ip 버킷 중 doc_count >= 20 이면 알럿
// Action: 해당 IP·실패 횟수를 메시지에 담아 통보
```

○ 저장검색
○ 알럿
● 임계치
○ 튜닝
○ 운영

S7

탐지 규칙·알럿·운영

공격 급증 임계치 규칙(DSL)

> 10분 창에서 critical 공격이 급증하면 즉시 알럿을 발생시킨다.

```
// 목표: 최근 10분간 critical 공격 급증 감지
// Monitor 실행 주기: 5분 (per query monitor)
{
  "query": {
    "bool": {
      "filter": [
        { "term":  { "event": "attack" } },
        { "range": { "@timestamp": { "gte": "now-10m" } } }
      ]
    }
  },
  "aggregations": {
    "critical_count": {
      "filter": { "term": { "severity": "critical" } }
    }
  }
}
// Trigger 조건: critical_count.doc_count >= 5 이면 알럿
// Action: attack_type 상위값과 총 critical 건수를 통보
```

○ 저장검색
○ 알럿
● 임계치
○ 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

임계치 설정 원리

> 임계치는 관측 창과 주기를 함께 정해야 의미가 생긴다.

임계 유형

- **절대 임계**: 5분 20회처럼 고정 횟수를 기준으로 삼아 규칙이 단순하고 이해하기 쉽다.
- **상대 임계**: 평소 baseline 대비 몇 배 급증했는지로 판정해 트래픽 규모 변화에 유연하게 대응한다.
- **조합**: 절대 하한과 상대 배수를 함께 걸어 저트래픽·고트래픽 상황을 모두 커버한다.

설정 요령 — 창·주기·throttle

- **보수적 시작**: 초기값은 다소 높게 잡아 오탐을 줄인 뒤 관측 데이터를 보며 점차 조정한다.
- **중복 억제**: throttle을 설정해 같은 조건의 알럿이 짧은 간격으로 반복 발송되지 않게 한다.

○ 저장검색
○ 알럿
● 임계치
○ 튜닝
○ 운영

오탐(False Positive)의 원인

> 오탐은 정상 활동을 위협으로 오인해 경보 신뢰를 갉아먹는다.

오탐 발생 원인

- **정상 자동화**: 배치 작업·헬스체크·검색엔진 크롤러가 반복 요청을 보내 임계치에 걸리는 경우가 많다.
- **넓은 쿼리**: 필터가 과도하게 포괄적이면 정상 트래픽까지 매칭돼 알럿이 남발된다.
- **낮은 임계치·부족한 맥락**: 임계치가 지나치게 낮거나 IP·계정 맥락이 없으면 정상도 위협으로 본다.

오탐의 비용

- **신뢰 하락**: 오탐이 잦으면 담당자가 알럿을 무시하기 시작해 진짜 위협까지 놓친다.
- **대응 낭비**: 허위 경보 조사에 인력·시간이 소모되어 실제 사고 대응 여력이 줄어든다.

○ 저장검색
○ 알럿
○ 임계치
● 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

튜닝 기법 — allowlist·baseline

> 알려진 정상은 제외하고 임계치는 데이터에 맞춰 동적으로 조정한다.

대표 기법

- **allowlist 제외**: 사내 모니터링 IP·정상 크롤러 UA를 규칙에서 예외 처리해 반복 오탐을 없앤다.
- **baseline 임계**: 평소 패턴을 기준선으로 삼아 그 대비 급증을 탐지하는 동적 임계로 전환한다.
- **시간 패턴 반영**: 업무 시간·주말 등 시간대·요일 특성을 반영해 시간대별로 다른 임계를 적용한다.

튜닝 절차 — 측정·조정·검증

- **측정 후 조정**: 실제 발생한 오탐을 집계해 원인을 확인하고 임계치·필터를 근거 있게 바꾼다.
- **회귀 검증**: 규칙을 버전 관리하고 과거 데이터로 재검증해 조정이 탐지력을 해치지 않았는지 확인한다.

○ 저장검색
○ 알럿
○ 임계치
● 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

알럿 피로 관리

> 과다한 알럿은 진짜 위협을 소음 속에 묻어버린다.

알럿 피로란

- **정의**: 지나치게 많은 알럿에 담당자가 둔감해져 중요한 경보까지 무시하게 되는 현상이다.
- **위험**: 하루 수백 건의 알럿 속에서 실제 침해 신호 한 건을 놓치면 대응이 지연된다.
- **원인**: 중복 알럿, 낮은 임계치, 심각도 구분 없는 일괄 통보가 피로를 가중한다.

완화 전략 — 우선순위·그룹핑

- **심각도 라우팅**: critical만 즉시 온콜로 보내고 낮은 심각도는 요약 리포트로 모아 전달한다.
- **상관·그룹핑**: 같은 IP·같은 규칙의 알럿을 묶고 자동 억제·정기 리뷰로 총량을 줄인다.

○ 저장검색
○ 알럿
○ 임계치
● 튜닝
○ 운영

S7
탐지 규칙·알럿·운영

운영 체크리스트

탐지 체계는 만든 뒤에도 주기적으로 점검해야 살아 있다.

항목	점검 내용	주기
인덱스 상태	_cat/indices로 상태·디스크 용량 확인, red 샤드 여부	일
수집 지연	최신 @timestamp가 현재와 근접한지 확인, 수집 중단 감지	일
규칙 상태	Monitor 활성 여부·실행 오류·마지막 실행 시각 점검	일
오탐률 리뷰	발생 알럿 대비 실제 위협 비율 집계·원인 분석	주
임계치 재보정	트래픽 변화 반영해 임계·allowlist 재조정	월
보존·롤오버	ILM 정책·인덱스 용량·롤오버 동작 점검	월

○ 저장검색
○ 알럿
○ 임계치
○ 튜닝
● 운영

S7

탐지 규칙·알럿·운영

세션 정리와 과정 마무리

> 저장 검색부터 운영까지, 그리고 과정 전체를 하나로 묶는다.

기억할 것

- **저장 검색**: 반복 탐지 쿼리를 저장 검색으로 만들어 재사용하고 알럿 규칙의 입력으로 승격한다.
- **임계치 규칙**: Monitor·Trigger·Action으로 브루트포스·공격 급증을 창·주기 기반 임계치로 자동 탐지한다.
- **튜닝·운영**: allowlist·baseline으로 오탐을 줄이고 체크리스트로 인덱스·규칙을 지속 점검한다.

과정 마무리와 다음 단계

- **전체 회고**: 수집→검색→시각화→관제→탐지→운영의 흐름을 하나의 파이프라인으로 완성했다.
- **다음 단계**: 자신의 로그를 이 랩에 적재해 실제 환경의 탐지 규칙과 대시보드로 확장해 본다.

○ 저장검색
○ 알럿
○ 임계치
○ 튜닝
● 운영