위협 탐지 시나리오

브루트포스 · 공격벡터 · 스캐너 · 데이터유출 · 지리이상

01
탐지 방법론
가설·쿼리·해석·대응 4단계 절차

02
인증·공격
브루트포스와 공격 벡터 집계

03
스캐너·유출
정찰 도구 탐지와 대량 응답 감시

04
지리·이상
지역 편중과 5xx 급증 신호

S6

위협 탐지 시나리오

세션 개요와 학습 목표

> 실제 로그에서 다섯 가지 공격 유형을 가설-쿼리-해석-대응 절차로 탐지한다.

이 세션에서 얻는 것

- **실전 탐지**: 브루트포스·공격벡터·스캐너·데이터유출·지리이상 다섯 시나리오를 순서대로 다뤄 손으로 찾아낸다.
- **공통 절차**: 모든 시나리오를 가설을 세우고 KQL로 증거를 모아 해석하고 대응하는 하나의 틀로 익힌다.
- **규칙화 연결**: 한 번 찾은 위협을 저장 검색·알럿으로 자동화해 다음 세션의 탐지 규칙으로 이어간다.

탐지의 마음가짐 — 가설 기반

- **의심에서 출발**: 무작정 로그를 훑지 않고 무엇을 의심하는지 가설을 먼저 세운 뒤 쿼리로 확인한다.
- **증거로 판단**: 감이 아니라 집계와 상위 값이라는 증거로 정상과 공격을 구분해 판단한다.

● 방법론
○ 브루트포스
○ 공격벡터
○ 스캐너·유출
○ 지리·정리

S6
위협 탐지 시나리오

탐지 방법론 — 가설·쿼리·해석·대응

> 네 단계를 반복하며 의심을 증거로, 증거를 대응으로 바꾼다.

4단계 절차

- **가설**: 무엇을 의심하는지 한 문장으로 정한다 — 예를 들어 한 IP가 로그인 실패를 반복하는지 묻는다.
- **쿼리**: KQL로 그 가설의 증거가 될 로그만 좁혀 수집한다 — event·필드 조건으로 범위를 한정한다.
- **해석**: 집계와 상위 값으로 편중을 읽어 정상 대비 이상 여부를 판단한다.
- **대응**: 차단·레이트리밋 등 조치를 취하고 재발을 막을 규칙으로 만든다.

반복 순환 — 탐지에서 튜닝으로

- **순환 구조**: 대응으로 끝이 아니라 오탐·미탐을 보고 가설과 쿼리를 다듬어 다시 돈다.
- **규칙 성장**: 반복할수록 임계치와 조건이 정교해져 자동 탐지 규칙의 품질이 올라간다.

● 방법론
○ 브루트포스
○ 공격벡터
○ 스캐너·유출
○ 지리·정리

S6
위협 탐지 시나리오

탐지 신호와 IOC

> 정상 baseline에서 벗어난 편차가 곧 탐지의 실마리다.

대표 신호

- **인증 실패 급증**: 한 IP나 계정에서 짧은 시간에 401 실패가 폭증하면 브루트포스를 의심한다.
- **비정상 UA·경로**: sqlmap 같은 도구 User-Agent나 /.env 같은 민감 경로 접근은 정찰 신호다.
- **대용량·이상 지역**: 평소보다 큰 정상 응답이나 대상국이 아닌 지역발 공격은 유출·지리이상을 시사한다.

baseline의 중요성

- **기준선 확보**: 평상시 실패율·응답 크기·지역 분포를 알아야 무엇이 비정상인지 편차로 잡아낸다.
- **IOC 활용**: 알려진 악성 IP·UA·경로를 침해 지표로 삼아 같은 흔적을 빠르게 검색한다.

● 방법론
○ 브루트포스
○ 공격벡터
○ 스캐너·유출
○ 지리·정리

S6
위협 탐지 시나리오

브루트포스 (1) 가설·쿼리

> 인증 실패를 좁힌 뒤 client_ip 상위 값으로 범인을 특정한다.

```
# 가설: 한 IP 가 짧은 시간에
#       로그인 실패를 반복한다
#       (크리덴셜 스터핑 후보)

# 1) 인증 실패 이벤트로 좁히기
event: auth_fail

# 2) 로그인 실패 POST 만
url: "/login" and http.method: POST
  and http.status: 401

# 3) admin 계정을 노린 실패
event: auth_fail and user: admin

# 4) 집계로 출발지 특정
#    Data Table → Terms
#    client_ip.keyword (Size 10)
#    → 실패 급증 상위 IP 확인
```

읽는 순서

- **가설**: 크리덴셜 스터핑으로 한 출발지가 다수 계정·비밀번호를 시도한다고 가정한다.
- **범위 축소**: auth_fail로 인증 실패만 남긴 뒤 client_ip 상위 값에서 편중을 확인한다.
- **계정 분포**: user별 실패 분포를 보면 특정 계정 집중인지 광범위 대입인지 드러난다.

○ 방법론
● 브루트포스
○ 공격벡터
○ 스캐너·유출
○ 지리·정리

S6
위협 탐지 시나리오

브루트포스 (2) 해석·대응

> 급증한 실패를 차단·잠금으로 막고 임계치 규칙으로 자동화한다.

해석 포인트

- **실패 편중**: 특정 IP나 계정에서 실패가 급증하면 정상 오타가 아니라 자동 대입 공격으로 본다.
- **패턴 확인**: 짧은 간격의 연속 실패, 다수 계정 순회, 동일 UA 반복은 브루트포스의 전형이다.
- **성공 여부**: 실패 뒤 200 성공이 섞이면 계정 탈취 성공을 의심해 우선순위를 높인다.

대응·규칙화

- **즉시 조치**: 해당 IP를 차단하고 레이트리밋·계정 잠금을 걸며 MFA로 재발을 막는다.
- **규칙화**: 저장 검색과 Alerting으로 임계치를 걸어 예를 들어 5분 20회 실패 시 자동 통보한다.

○ 방법론
● 브루트포스
○ 공격벡터
○ 스캐너·유출
○ 지리·정리

S6

위협 탐지 시나리오

공격 벡터 집계 (쿼리)

공격 이벤트를 유형·심각도별로 집계해 최다 벡터를 찾는다.

```
# 1) 공격 이벤트로 범위 한정
event: attack

# 2) 공격 유형별 분포
#    Vertical Bar → X-axis
#    Terms → attack_type.keyword
#    → 가장 많은 공격 벡터 확인

# 3) 심각도 높은 공격만
severity: (high or critical)

# 4) 특정 유형 파고들기
event: attack and attack_type: sqli

# 5) 상위 공격자 집계
#    Data Table → Terms
#    client_ip.keyword (Size 10)
```

읽는 순서

- **범위 한정**: event:attack으로 공격 이벤트만 남겨 집계 대상을 명확히 한다.
- **최다 벡터**: attack_type을 Terms로 집계해 가장 많이 시도된 공격 유형을 파악한다.
- **우선순위**: severity로 critical 비중을 보고 먼저 대응할 위협을 정한다.

○ 방법론
○ 브루트포스
● 공격벡터
○ 스캐너·유출
○ 지리·정리

S6
위협 탐지 시나리오

공격 벡터 해석·대응

> 최다 벡터와 심각도로 패치·차단의 우선순위를 결정한다.

해석 포인트

- **최다 벡터**: sqli·xss·path_traversal·cmd_injection 중 어떤 유형이 가장 많은지로 방어 초점을 잡는다.
- **심각도 비중**: 전체 공격 중 critical이 차지하는 비율이 높으면 즉각 대응이 필요한 상황이다.
- **출발지 상관**: 특정 IP가 여러 벡터를 섞어 시도하면 조직적 공격으로 보고 함께 차단한다.

대응 우선순위

- **취약점 패치**: 최다 벡터가 겨냥한 취약점을 먼저 패치해 실제 노출 면을 줄인다.
- **WAF·차단**: 해당 유형의 WAF 룰을 강화하고 반복 공격자 IP를 차단해 시도를 막는다.

○ 방법론
○ 브루트포스
● 공격벡터
○ 스캐너·유출
○ 지리·정리

S6

위협 탐지 시나리오

취약점 스캐너 탐지

> 자동화 도구 UA와 민감 경로 접근을 정찰 신호로 잡는다.

```
# 1) 스캐너 도구 User-Agent
user_agent: *sqlmap*
  or user_agent: *nikto*

# 2) 민감 경로 스캔 시도
url: *.env* or url: *wp-login*

# 3) 범용 자동화 클라이언트
user_agent: *python-requests*
  or user_agent: *curl*

# 4) 도구 + 경로 결합(정찰 확정)
(user_agent: *sqlmap* or url: *.env*)

# 5) 출발지 특정
#    Terms → client_ip.keyword
#    → 정찰 IP 목록화
```

읽는 순서

- **정찰 신호**: 자동화 도구 UA와 민감 경로 접근이 겹치면 공격 전 정찰 단계로 판단한다.
- **출발지 특정**: client_ip로 어느 IP가 스캔을 돌리는지 특정해 목록으로 만든다.
- **조기 차단**: 정찰 단계에서 미리 차단하면 본격 공격으로의 진행을 끊을 수 있다.

○ 방법론
○ 브루트포스
○ 공격벡터
● 스캐너·유출
○ 지리·정리

S6

위협 탐지 시나리오

○ 방법론
○ 브루트포스
○ 공격벡터
● 스캐너·유출
○ 지리·정리

데이터 유출 의심

평소보다 큰 정상 응답이 한곳에 몰리면 대량 반출을 의심한다.

```
# 1) 대용량 정상 응답
http.status: 200
  and http.bytes > 30000

# 2) 특정 IP 로 좁혀 확인
http.status: 200
  and http.bytes > 30000
  and client_ip: "10.0.0.9"

# 3) 응답 시간 병행 점검
#    response_ms 컬럼 추가
#    → 큰 응답 + 긴 시간 = 덤프 의심

# 4) 경로별 집계
#    Terms → url.keyword
#    → 어느 경로에 몰리는지 확인
```

읽는 순서

- **대량 반출**: 정상 200 응답이라도 bytes가 특정 IP·경로에 몰리면 대량 다운로드나 덤프를 의심한다.
- **시간 상관**: response_ms를 함께 보면 큰 응답에 긴 처리 시간이 붙는 반출 패턴이 드러난다.
- **경로 확인**: url별 집계로 어떤 엔드포인트가 유출 통로인지 좁힌다.

S6
위협 탐지 시나리오

데이터 유출 분석 심화

> baseline 대비 편차와 반복 패턴으로 유출을 확정하고 대응한다.

이상 판단 기준

- **bytes 편차**: 평소 응답 크기 baseline과 비교해 크게 벗어난 응답을 이상치로 표시한다.
- **반복 패턴**: 같은 IP가 큰 응답을 짧은 간격으로 반복 수신하면 단발 조회가 아닌 반출로 본다.
- **계정·경로 상관**: 인증 계정과 접근 경로를 엮어 권한을 벗어난 대량 접근인지 확인한다.

대응

- **세션 차단**: 의심 세션과 계정을 즉시 차단하고 관련 IP를 격리한다.
- **DLP·감사**: DLP 정책으로 반출을 막고 접근 감사 로그로 유출 범위를 조사한다.

○ 방법론
○ 브루트포스
○ 공격벡터
● 스캐너·유출
○ 지리·정리

S6

위협 탐지 시나리오

지리·이상 징후

대상국이 아닌 지역발 공격 집중과 5xx 급증을 함께 감시한다.

```
# 1) 특정 지역발 공격 집중
geo.country: (RU or CN)
  and event: attack

# 2) 단일 국가로 좁히기
geo.country: RU and event: attack

# 3) 서버 오류(5xx) 급증
http.status >= 500

# 4) Region Map 연계
#    Terms → geo.country.keyword
#    Join field → iso2
#    → 접속·공격 지역을 지도로

# 5) 시간 추이와 상관
#    Line → Date Histogram
#    → 급증 구간 포착
```

읽는 순서

- **지역 편중**: 서비스 대상국이 아닌 지역에서 공격이 몰리면 지오펜싱 도입을 검토한다.
- **지도 확인**: Region Map으로 국가별 접속·공격량을 색으로 보면 편중이 한눈에 드러난다.
- **5xx 신호**: 5xx 급증은 DoS나 애플리케이션 오작동의 조기 신호로 함께 살핀다.

○ 방법론

○ 브루트포스

○ 공격벡터

○ 스캐너·유출

● 지리·정리

S6
위협 탐지 시나리오

5xx 급증과 오작동·DoS 신호

> 5xx 급증이 배포 탓인지 공격 탓인지 추이로 구분해 대응한다.

5xx 해석

- **이중 원인**: http.status 500 이상 급증은 애플리케이션 오류일 수도, DoS로 인한 과부하일 수도 있다.
- **추이 상관**: Line 트래픽 추이와 겹쳐 보면 요청 폭증에 동반된 5xx인지 내부 오류인지 갈린다.
- **배포 구분**: 정상 배포 직후의 일시적 오류와 지속적인 이상 오류를 시간대로 구분한다.

대응 판단

- **부하 대응**: 트래픽 폭증이면 스케일 아웃이나 레이트리밋으로 완화하고 공격원을 차단한다.
- **오류 대응**: 배포 결함이면 롤백으로 되돌리고 원인 커밋을 추적해 수정한다.

○ 방법론
○ 브루트포스
○ 공격벡터
○ 스캐너·유출
● 지리·정리

S6

위협 탐지 시나리오

세션 정리와 다음 예고

> 다섯 시나리오를 하나의 절차로 묶어 정리하고 규칙화로 잇는다.

기억할 것

- **공통 절차**: 브루트포스·공격벡터·스캐너·유출·지리이상 모두 가설-쿼리-해석-대응 한 틀로 탐지했다.
- **증거 중심**: event로 좁히고 Terms 상위 값과 집계로 편중을 읽어 정상과 공격을 갈랐다.
- **대응 연결**: 차단·패치·격리로 끝내지 않고 저장 검색과 임계치 규칙으로 자동화까지 이었다.

다음 예고 — 세션 7

- **탐지 규칙**: 이번에 찾은 시나리오를 저장 검색과 알럿 규칙으로 정식화한다.
- **운영**: 임계치 튜닝·오탐 관리·통보 채널까지 관제 운영의 흐름을 익힌다.

○ 방법론
○ 브루트포스
○ 공격벡터
○ 스캐너·유출
● 지리·정리