### Event 필드

event 필드는 로그 또는 메트릭 이벤트 자체에 대한 컨텍스트 정보에 사용됩니다.

로그는 발생한 일에 대한 세부 정보가 포함된 이벤트로 정의됩니다. 로그 이벤트에는 어떤 일이 발생한 시간이 포함되어야 합니다. 로그 이벤트의 예로는 호스트에서 프로세스 시작, 소스에서 대상으로 전송되는 네트워크 패킷, 클라이언트와 서버 간의 네트워크 연결이 시작되거나 종료되는 것 등이 있습니다. 메트릭은 하나 이상의 수치 측정값과 측정이 수행된 시간을 포함하는 이벤트로 정의됩니다. 메트릭 이벤트의 예로는 호스트에서 측정된 메모리 사용율, 디바이스 온도 등이 있습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| event.action | action | 문자열 | 예: group-add, process-started, file-created |
| event.agent\_id\_status | agent\_id\_status | 문자열 | 예: verified, mismatch, missing, auth\_metadata\_missing |
| event.category | category | 문자열 | 예: api, authentication, configuration, database, driver, email, file, host, iam, intrusion\_detection, library, malware, network, package, process, registry, session, threat, vulnerability, web |
| event.code | event\_code | 문자열 | 예: 윈도우 이벤트 ID |
| event.created | event\_created | 날짜 | 이벤트를 에이전트가 수집한 시각 |
| event.dataset | event\_dataset | 문자열 | 데이터셋 이름. 예: apache.access |
| event.duration | duration | 64비트 실수 | 이벤트 지속 시간. 원본은 나노초 단위이며 초 단위 변환 필요 |
| event.end | last\_seen | 날짜 | 이벤트 최근 발견 시점 |
| event.hash | event\_hash | 문자열 | 로그 무결성 검증에 필요한 해시 |
| event.id | event\_uid | 문자열 | 이벤트 유일 식별자 |
| event.ingested | event\_ingested | 날짜 | 데이터가 중앙 클러스터에 유입된 시점 |
| event.kind | event\_kind | 문자열 | 예: alert, asset, enrichment, event, metric, state, pipeline\_error, signal |
| event.module | event\_module | 문자열 | 예: apache |
| event.original | line | 문자열 | 원본 로그 메시지 |
| event.outcome | outcome | 문자열 | 예: failure, success, unknown |
| event.provider | event\_provider | 문자열 | 예: kernel, Microsoft-Windows-Security-Auditing |
| event.reason | reason | 문자열 | 이벤트 발생 사유. 예: blocked site |
| event.reference | reference | 문자열 | 이벤트 정의에 대한 추가 정보 URL |
| event.risk\_score | risk\_score | 64비트 실수 | 위험 점수 또는 우선순위 |
| event.risk\_score\_norm | risk\_score\_norm | 64비트 실수 | 0-100 범위로 정규화된 위험 점수 |
| event.sequence | event\_seq | 64비트 정수 | 이벤트 일련번호 |
| event.severity | severity | 32비트 정수 | 0(unusable)-7(debug) 범위의 위험도 |
| event.start | first\_seen | 날짜 | 이벤트 최초 발견 시점 |
| event.timezone | timezone | 문자열 | 예: Europe/Amsterdam, EST, -05:00 |
| event.type | event\_type | 문자열 | 예: access, admin, allowed, change, connection, creation, deletion, denied, end, error, group, indicator, info, installation, protocol, start, user |
| event.url | external\_url | 문자열 | 외부 시스템으로 연결되는 이벤트 URL |