### Rule 필드

rule 필드는 알림이나 경보를 생성하는 관찰자 또는 에이전트 규칙의 세부 정보를 표시하는데 사용됩니다.

rule 필드를 채우는 데이터 소스의 예로는 NAC, 네트워크 또는 호스트 IDS/IPS, 네트워크 방화벽, 웹 방화벽, URL 필터, 엔드포인트 탐지 및 대응(EDR) 시스템 등이 있습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| rule.author | rule\_author | 문자열 | 룰 작성자 |
| rule.category | category | 문자열 | 룰 분류. 예: Attempted Information Leak |
| rule.description | description | 문자열 | 룰 설명. 예: Block requests to public DNS over HTTPS / TLS protocols |
| rule.id | sid | 문자열 | 룰 ID. 예: 101 |
| rule.license | rule\_license | 문자열 | 룰 라이선스. 예: Apache 2.0 |
| rule.name | rule\_name | 문자열 | 룰 또는 시그니처 이름. 예: BLOCK\_DNS\_over\_TLS |
| rule.reference | reference | 문자열 | 레퍼런스 URL. 예: https://en.wikipedia.org/wiki/DNS\_over\_TLS |
| rule.ruleset | policy | 문자열 | 룰 집합, 정책, 그룹, 상위 분류 이름. 예: Standard\_Protocol\_Filters |
| rule.uuid | rule\_uuid | 문자열 | 룰 식별자 |
| rule.version | rule\_ver | 문자열 | 룰 버전 |