### File 필드

file 필드는 파일 시스템에서 생성되었거나 파일 시스템에 존재했던 정보의 집합으로 정의됩니다.

파일 개체는 호스트 이벤트, 네트워크 이벤트 및/또는 파일 이벤트(예: 파일 무결성 모니터링 제품 또는 서비스에서 생성된 이벤트)와 연결될 수 있습니다. 파일 필드는 이벤트 또는 메트릭과 관련된 영향을 받는 파일에 대한 세부 정보를 제공합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| file.accessed | file\_atime | 날짜 | 파일 최근 접근 시각 |
| file.attributes | file\_attrs | 문자열 | 파일 특성 목록. 예: readonly, system |
| file.created | file\_ctime | 날짜 | 파일 생성 시각 |
| file.ctime | file\_ctime | 날짜 | 파일 생성 시각 |
| file.device | file\_device | 문자열 | 파일이 저장된 스토리지 장치 이름. 예: sda |
| file.directory | file\_dir | 문자열 | 파일이 저장된 디렉터리 절대 경로 |
| file.drive\_letter | drive\_letter | 문자열 | 윈도우 드라이브 문자. 예: C |
| file.extension | file\_ext | 문자열 | 파일 확장자. 예: png |
| file.fork\_name | ads\_name | 문자열 | NTFS ADS 이름. 예: Zone.Identifer |
| file.gid | file\_gid | 문자열 | 파일 소유자 그룹 ID |
| file.group | file\_group | 문자열 | 파일 소유자 그룹 이름 |
| file.inode | file\_inode | 문자열 | 파일 Inode |
| file.mime\_type | file\_mime\_type | 문자열 | 파일 MIME 유형 |
| file.mode | file\_mode | 문자열 | 8진수 퍼미션 |
| file.mtime | file\_mtime | 날짜 | 파일 최근 수정 시각 |
| file.name | file\_name | 문자열 | 파일 이름 |
| file.owner | file\_owner | 문자열 | 파일 소유자 계정 이름 |
| file.path | file\_path | 문자열 | 파일 절대 경로 |
| file.size | file\_size | 64비트 정수 | 파일 크기 |
| file.target\_path | target\_path | 문자열 | 심볼릭 링크의 대상 경로 |
| file.type | file\_type | 문자열 | 파일 유형. 예: file, dir, symlink |
| file.uid | file\_uid | 문자열 | 파일 소유자의 UID 또는 SID |