### Observer 필드

옵저버는 네트워크, 보안 또는 애플리케이션 관련 이벤트 및 메트릭을 감지, 관찰 또는 생성하는 데 사용되는 특수 네트워크, 보안 또는 애플리케이션 디바이스로 정의됩니다.

이는 사용자 지정 하드웨어 어플라이언스 또는 특수 네트워크, 보안 또는 애플리케이션 소프트웨어를 실행하도록 구성된 서버일 수 있습니다. 예를 들어 방화벽, 웹 프록시, 침입방지 시스템, 네트워크 모니터링 센서, 웹 방화벽, 데이터유출방지(DLP), APM 서버 등이 있습니다.

observer 필드에는 네트워크, 보안 또는 애플리케이션 이벤트 또는 메트릭을 감지, 관찰, 생성하는 시스템의 세부 정보를 입력해야 합니다. 이벤트 또는 메트릭 처리에 사용되는 메시지 큐와 ETL 구성 요소는 ECS에서 관찰자로 간주되지 않습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| observer.egress.zone | dst\_zone | 문자열 | 목적지 네트워크 영역. 예: Internal, External, DMZ, HR, Legal |
| observer.hostname | device\_name | 문자열 | 옵저버 호스트명 |
| observer.ingress.zone | src\_zone | 문자열 | 출발지 네트워크 영역. 예: internal, External, DMZ, HR, Legal |
| observer.ip | device\_ip | IP 주소 | 옵저버 IP 주소 |
| observer.mac | device\_mac | 문자열 | 옵저버 MAC 주소 |
| observer.name | device\_name | 문자열 | 옵저버 사용자 정의 이름 |
| observer.product | product | 문자열 | 옵저버 제품 이름 |
| observer.serial\_number | device\_serial | 문자열 | 옵저버 제품 일련번호 |
| observer.type | device\_type | 문자열 | 옵저버 데이터 유형 |
| observer.vendor | vendor | 문자열 | 옵저버 제조사 이름 |
| observer.version | ver | 문자열 | 옵저버 버전 |