### Network 필드

네트워크는 호스트 또는 네트워크 이벤트가 발생하는 통신 경로로 정의됩니다. network 필드는 이벤트와 관련된 네트워크 활동에 대한 세부 정보로 채워야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| network.application | app | 문자열 | 웹 애플리케이션. 예: facebook, twitter |
| network.bytes | total\_bytes | 64비트 정수 | 총 전송 바이트 수 (양방향) |
| network.community\_id | community\_id | 문자열 | 커뮤니티 ID. 예: 1:hO+sN4H+MG5MY/8hIrXPqc4ZQz0= |
| network.direction | direction | 문자열 | 통신 방향. 예: inbound, outbound, internal, external, unknown |
| network.forwarded\_ip | forwarded\_ip | IP 주소 | 출발지가 프록시인 경우 원본 호스트 IP 주소 |
| network.packets | total\_pkts | 64비트 정수 | 총 전송 패킷 수 (양방향) |
| network.protocol | app | 문자열 | L7 애플리케이션. 예: http, dns, ssh |
| network.transport | protocol | 문자열 | L4 프로토콜. 예: UDP, TCP, IPV6-ICMP |
| network.type | net\_type | 문자열 | 네트워크 계층 유형. 예: ipv4, ipv6, ipsec, pim |