## ECS 개요

Elastic은 이벤트를 분석, 시각화, 상호 연관시키기 용이하도록 ECS(Elastic Common Schema)에 맞춰 데이터를 정규화합니다. 특히 Elastic Observability 또는 Elastic Security와 같은 Elastic 솔루션을 사용하는 경우, 모든 이벤트가 ECS에 매핑됩니다.

예를 들어, 아래와 같은 웹 로그를 ECS에 매핑하여 볼 수 있습니다:

10.42.42.42 - - [15/Jul/2020:20:48:32 +0000] "GET /content HTTP/1.1" 200 2571 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36

|  |  |
| --- | --- |
| ECS 필드 | 값 |
| @timestamp | 2020-07-15T20:48:32.000Z |
| ecs.version | 8.11 |
| event.module | apache |
| event.dataset | apache.access |
| event.kind | event |
| event.category | "network", "web" |
| event.type | "access" |
| event.outcome | success |
| event.original | 웹 로그 원본 문자열 |
| http.request.method | GET |
| http.response.body.bytes | 2571 |
| http.response.status\_code | 200 |
| http.version | 1.1 |
| source.address | 10.42.42.42 |
| source.ip | 10.42.42.42 |
| url.original | /content |
| user\_agent.original | Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36 |

Elastic은 주로 JSON 형식으로 데이터를 관리하므로 필드가 그룹화되어 있습니다. 로그프레소 플랫폼은 복합 객체를 지원하지만 로그프레소 고유의 정규화 기준이 있으므로, Elastic 데이터를 수신하는 경우 로그프레소 필드 이름으로 정규화하는 것을 권장합니다.

[Elasticsearch 앱](https://logpresso.store/ko/apps/elasticsearch)에 내장된 elastic 파서는 ECS 8.11 스키마에 맞는 JSON 데이터를 파싱하여 자동으로 로그프레소 정규화 기준에 맞게 변환합니다.