Elastic Common Schema 정규화

## 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.

### Base 필드

base 필드 집합은 모든 Elastic 이벤트에 공통적으로 사용되는 필드입니다. 각 base 필드는 아래와 같이 로그프레소 필드 이름으로 변환합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| @timestamp | event\_time | 날짜 | 이벤트 최초 생성 시각 |
| message | msg | 문자열 | 로그 뷰어에 표시할 메시지 |
| tags | tags | 리스트 | 태그 목록 |
| labels | labels | 리스트 | 사용자 정의 키/값 쌍 |

### Client 필드

클라이언트는 세션, 연결 또는 양방향 플로우 레코드와 관련된 이벤트에 대한 네트워크 연결의 개시자로 정의됩니다.

TCP 이벤트의 경우, 클라이언트는 SYN 패킷을 전송하는 TCP 연결의 개시자입니다. 다른 프로토콜의 경우, 클라이언트는 일반적으로 네트워크 트랜잭션의 개시자 또는 요청자입니다. 일부 시스템에서는 TCP 연결에서 클라이언트를 지칭하기 위해 "발신자"라는 용어를 사용합니다. 클라이언트 필드는 네트워크 이벤트에서 클라이언트 역할을 하는 시스템에 대한 세부 정보를 설명합니다. client 필드는 일반적으로 server 필드와 함께 채워집니다. 클라이언트 필드는 일반적으로 패킷 수준 이벤트에 대해 채워지지 않습니다.

클라이언트/서버 표현은 특정 상황에서 데이터를 시각화하는 데 도움이 되는 의미론적 컨텍스트를 교환에 추가할 수 있습니다. 컨텍스트가 해당 범주에 속하는 경우에도 소스 및 목적지가 적절하게 채워져 있는지 확인해야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| client.address | src\_addr | 문자열 | 클라이언트 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| client.bytes | sent\_bytes | 64비트 정수 | 클라이언트가 서버로 전송한 바이트 수 |
| client.domain | src\_host | 문자열 | 클라이언트 도메인 이름 |
| client.ip | src\_ip | IP 주소 | 클라이언트 IP 주소 (IPv4 또는 IPv6) |
| client.mac | src\_mac | 문자열 | 클라이언트 MAC 주소 |
| client.nat.ip | nat\_src\_ip | IP 주소 | NAT 출발지 주소 |
| client.nat.port | nat\_src\_port | 32비트 정수 | NAT 출발지 포트 |
| client.packets | rcvd\_pkts | 64비트 정수 | 클라이언트가 서버로 전송한 패킷 수 |
| client.port | src\_port | 32비트 정수 | 클라이언트 포트 |
| client.registered\_domain | src\_eld | 문자열 | 출발지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| client.subdomain | src\_subdomain | 문자열 | 출발지 서브도메인 |
| client.top\_level\_domain | src\_tld | 문자열 | 출발지 TLD |

### Destination 필드

destination 필드는 네트워크 교환/패킷의 수신자에 대한 세부 정보를 캡처합니다. 이러한 필드는 네트워크 이벤트, 패킷 또는 네트워크 트랜잭션의 세부 정보가 포함된 기타 이벤트에서 채워집니다.

destination 필드는 일반적으로 source 필드와 함께 채워집니다. source 및 destination 필드는 기본 요소이므로 이벤트에 네트워크 트랜잭션의 소스 및 대상 세부 정보가 포함된 경우 항상 채워져야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| destination.address | dst\_addr | 문자열 | 목적지 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| destination.bytes | rcvd\_bytes | 64비트 정수 | 목적지에서 출발지로 전송한 바이트 수 |
| destination.domain | dst\_host | 문자열 | 목적지 도메인 이름 |
| destination.ip | dst\_ip | IP 주소 | 목적지 IP 주소 (IPv4 또는 IPv6) |
| destination.mac | dst\_mac | 문자열 | 목적지 MAC 주소 |
| destination.nat.ip | nat\_dst\_ip | IP 주소 | NAT 목적지 IP 주소 |
| destination.nat.port | nat\_dst\_port | 32비트 정수 | NAT 목적지 포트 |
| destination.packets | rcvd\_pkts | 64비트 정수 | 목적지에서 출발지로 전송한 패킷 수 |
| destination.port | dst\_port | 32비트 정수 | 목적지 포트 |
| destination.registered\_domain | dst\_eld | 문자열 | 목적지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| destination.subdomain | dst\_subdomain | 문자열 | 목적지 서브도메인 |
| destination.top\_level\_domain | dst\_tld | 문자열 | 목적지 TLD |
| destination.user.domain | dst\_nt\_domain | 문자열 | 목적지 계정이 속한 액티브 디렉터리 또는 LDAP 도메인 이름. |
| destination.user.email | mail\_to | 문자열 | 목적지 계정 이메일 |
| destination.user.full\_name | dst\_emp\_name | 문자열 | 목적지 사용자 성명 |
| destination.user.hash | dst\_user\_hash | 문자열 | 목적지 계정 익명화 필요 시 계정 해시 값 |
| destination.user.id | dst\_user\_id | 문자열 | 목적지 계정 식별자. 예: S-1-5-21-202424912787-2692429404-2351956786-1000 |
| destination.user.name | dst\_user | 문자열 | 목적지 로그인 이름 |
| destination.user.roles | dst\_user\_roles | 리스트 | 이벤트 발생 시점에 목적지 사용자가 보유한 역할 목록 |

### DLL 필드

dll 필드에는 프로세스에 동적으로 로드되는 코드 라이브러리에 대한 정보가 포함되어 있습니다.

많은 운영 체제에서 서로 다른 이름의 "공유 코드 라이브러리"를 참조하지만 이 필드 집합은 다음 모두를 참조합니다:

* Windows에서 일반적으로 사용되는 동적 링크 라이브러리 (.dll)
* 유닉스 계열 운영 체제에서 일반적으로 사용되는 공유 객체 (.so)
* macOS에서 일반적으로 사용되는 동적 라이브러리 (.dylib)

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| dll.name | dll\_name | 문자열 | 라이브러리 이름. 예: kernel32.dll |
| dll.path | dll\_path | 문자열 | 라이브러리 파일 경로. 예: C:\Windows\System32\kernel32.dll |

### ECS 필드

ECS 메타 정보를 정의합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| ecs.version | ecs\_ver | 문자열 | 모든 이벤트는 어떤 ECS 스키마 버전에 호환되는지 명시해야 함 |

### Event 필드

event 필드는 로그 또는 메트릭 이벤트 자체에 대한 컨텍스트 정보에 사용됩니다.

로그는 발생한 일에 대한 세부 정보가 포함된 이벤트로 정의됩니다. 로그 이벤트에는 어떤 일이 발생한 시간이 포함되어야 합니다. 로그 이벤트의 예로는 호스트에서 프로세스 시작, 소스에서 대상으로 전송되는 네트워크 패킷, 클라이언트와 서버 간의 네트워크 연결이 시작되거나 종료되는 것 등이 있습니다. 메트릭은 하나 이상의 수치 측정값과 측정이 수행된 시간을 포함하는 이벤트로 정의됩니다. 메트릭 이벤트의 예로는 호스트에서 측정된 메모리 사용율, 디바이스 온도 등이 있습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| event.action | action | 문자열 | 예: group-add, process-started, file-created |
| event.agent\_id\_status | agent\_id\_status | 문자열 | 예: verified, mismatch, missing, auth\_metadata\_missing |
| event.category | category | 문자열 | 예: api, authentication, configuration, database, driver, email, file, host, iam, intrusion\_detection, library, malware, network, package, process, registry, session, threat, vulnerability, web |
| event.code | event\_code | 문자열 | 예: 윈도우 이벤트 ID |
| event.created | event\_created | 날짜 | 이벤트를 에이전트가 수집한 시각 |
| event.dataset | event\_dataset | 문자열 | 데이터셋 이름. 예: apache.access |
| event.duration | duration | 64비트 실수 | 이벤트 지속 시간. 원본은 나노초 단위이며 초 단위 변환 필요 |
| event.end | last\_seen | 날짜 | 이벤트 최근 발견 시점 |
| event.hash | event\_hash | 문자열 | 로그 무결성 검증에 필요한 해시 |
| event.id | event\_uid | 문자열 | 이벤트 유일 식별자 |
| event.ingested | event\_ingested | 날짜 | 데이터가 중앙 클러스터에 유입된 시점 |
| event.kind | event\_kind | 문자열 | 예: alert, asset, enrichment, event, metric, state, pipeline\_error, signal |
| event.module | event\_module | 문자열 | 예: apache |
| event.original | line | 문자열 | 원본 로그 메시지 |
| event.outcome | outcome | 문자열 | 예: failure, success, unknown |
| event.provider | event\_provider | 문자열 | 예: kernel, Microsoft-Windows-Security-Auditing |
| event.reason | reason | 문자열 | 이벤트 발생 사유. 예: blocked site |
| event.reference | reference | 문자열 | 이벤트 정의에 대한 추가 정보 URL |
| event.risk\_score | risk\_score | 64비트 실수 | 위험 점수 또는 우선순위 |
| event.risk\_score\_norm | risk\_score\_norm | 64비트 실수 | 0-100 범위로 정규화된 위험 점수 |
| event.sequence | event\_seq | 64비트 정수 | 이벤트 일련번호 |
| event.severity | severity | 32비트 정수 | 0(unusable)-7(debug) 범위의 위험도 |
| event.start | first\_seen | 날짜 | 이벤트 최초 발견 시점 |
| event.timezone | timezone | 문자열 | 예: Europe/Amsterdam, EST, -05:00 |
| event.type | event\_type | 문자열 | 예: access, admin, allowed, change, connection, creation, deletion, denied, end, error, group, indicator, info, installation, protocol, start, user |
| event.url | external\_url | 문자열 | 외부 시스템으로 연결되는 이벤트 URL |

### 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 |

### Geo 필드

geo 필드에는 이벤트와 관련된 특정 위치에 대한 데이터가 포함될 수 있습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| geo.city\_name | city | 문자열 | 도시 이름. 예: Montreal |
| geo.continent\_code | continent\_code | 문자열 | ISO 2문자 대륙 코드. 예: NA |
| geo.continent\_name | continent\_name | 문자열 | 대륙 이름. 예: North America |
| geo.country\_iso\_code | country | 문자열 | ISO 2문자 국가 코드. 예: CA |
| geo.country\_name | country\_name | 문자열 | 국가 이름. 예: Canada |
| geo.location.lon | lng | 64비트 정수 | 경도 |
| geo.location.lat | lat | 64비트 정수 | 위도 |
| geo.name | location | 문자열 | 사용자 정의 위치 이름 |
| geo.postal\_code | postal\_code | 문자열 | 우편 번호 |
| geo.region\_iso\_code | region\_code | 문자열 | ISO 지역 코드 |
| geo.region\_name | region\_name | 문자열 | 지역 이름 |
| geo.timezone | timezone | 문자열 | 시간대 |

### Hash 필드

hash 필드는 서로 다른 비트 단위 해시 알고리즘과 그 값을 나타냅니다. ja3 또는 imphash와 같은 특수 목적의 해시는 해당 해시와 관련된 필드 집합(각각 tls 및 pe)에 배치됩니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| hash.md5 | md5 | 문자열 | MD5 해시 |
| hash.sha1 | sha1 | 문자열 | SHA1 해시 |
| hash.sha256 | sha256 | 문자열 | SHA256 해시 |
| hash.sha384 | sha384 | 문자열 | SHA384 해시 |
| hash.sha512 | sha512 | 문자열 | SHA512 해시 |
| hash.ssdeep | ssdeep | 문자열 | SSDEEP 해시 |
| hash.tlsh | tlsh | 문자열 | TLSH 해시 |

### HTTP 필드

HTTP 통신과 관련된 필드입니다. HTTP 요청의 URL은 url 필드 집합을 사용하여 표현합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| http.request.body.bytes | http\_req\_body\_bytes | 64비트 정수 | HTTP 요청 본문의 바이트 수 |
| http.request.body.content | http\_req\_body | 문자열 | HTTP 요청 본문 내용 |
| http.request.bytes | cs\_bytes | 64비트 정수 | HTTP 요청 바이트 수 (헤더 및 바디) |
| http.request.id | http\_req\_id | 문자열 | HTTP 요청 식별자. X-Request-ID 또는 X-Correlation-ID 헤더 |
| http.request.method | method | 문자열 | HTTP 요청 메소드 |
| http.request.mime\_type | http\_req\_content\_type | 문자열 | HTTP 요청 MIME 유형. 예: image/gif |
| http.request.referrer | referer | 문자열 | HTTP 요청 레퍼러 |
| http.response.body.bytes | http\_resp\_body\_bytes | 64비트 정수 | HTTP 응답 본문의 바이트 수 |
| http.response.body.content | http\_resp\_body | 문자열 | HTTP 응답 본문 내용 |
| http.response.bytes | sc\_bytes | 64비트 정수 | HTTP 응답 바이트 수 (헤더 및 바디) |
| http.response.mime\_type | http\_resp\_content\_type | 문자열 | HTTP 응답 MIME 유형. 예: image/gif |
| http.response.status\_code | status | 32비트 정수 | HTTP 응답 상태 코드. 예: 404 |
| http.version | http\_ver | 문자열 | HTTP 버전. 예: 1.1 |

### 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 |

### 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 |

### Operating System 필드

os 필드는 운영체제와 관련된 정보를 포함합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| os.family | os\_family | 문자열 | 운영체제 계열. 예: redhat, debian, freebsd, windows |
| os.full | os\_full | 문자열 | 운영체제 전체 이름. 예: Mac OS Mojave |
| os.kernel | os\_kernel | 문자열 | 운영체제 커널. 예: 4.4.0-112-generic |
| os.name | os\_name | 문자열 | 운영체제 이름. 예: Mac OS X |
| os.platform | os\_platform | 문자열 | 운영체제 플랫폼. 예: centos, ubuntu, windows, darwin |
| os.type | os\_type | 문자열 | 운영체제 유형. 예: linux, macos, unix, windows, ios, android |
| os.version | os\_ver | 문자열 | 운영체제 버전. 예: 10.14.1 |

### Related 필드

related 필드는 연관 분석에 필요한 식별자를 제공합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| related.hash | related\_hash | 문자열 | 이벤트에서 발견된 모든 해시 목록 (MD5, SHA1 등) |
| related.hosts | rlated\_hosts | 문자열 | 이벤트에서 발견된 몯느 호스트명 또는 도메인 목록 |
| related.ip | related\_ips | 문자열 | 이벤트에서 발견된 모든 IP 주소 목록 |
| related.user | related\_users | 문자열 | 이벤트에서 발견된 모든 계정 목록 |

### 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 |

### Server 필드

서버는 세션, 연결 또는 양방향 플로우 레코드와 관련된 이벤트에 대한 네트워크 연결에서 응답자로 정의됩니다.

TCP 이벤트의 경우, 서버는 TCP 연결의 초기 SYN 패킷을 수신합니다. 다른 프로토콜의 경우 서버는 일반적으로 네트워크 트랜잭션에서 응답자입니다. 일부 시스템은 실제로 TCP 연결에서 서버를 지칭하기 위해 "응답자"라는 용어를 사용합니다. 서버 필드는 네트워크 이벤트에서 서버 역할을 하는 시스템에 대한 세부 정보를 설명합니다. 서버 필드는 일반적으로 클라이언트 필드와 함께 채워집니다. 서버 필드는 일반적으로 패킷 수준 이벤트에 대해 채워지지 않습니다.

클라이언트/서버 표현은 특정 상황에서 데이터를 시각화하는 데 도움이 되는 의미론적 컨텍스트를 교환에 추가할 수 있습니다. 컨텍스트가 해당 범주에 속하는 경우에도 출발지 및 목적지가 적절하게 채워져 있는지 확인해야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| server.address | dst\_addr | 문자열 | 서버 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| server.bytes | rcvd\_bytes | 64비트 정수 | 서버가 클라이언트로 전송한 바이트 수 |
| server.domain | dst\_host | 문자열 | 서버 도메인 이름 |
| server.ip | dst\_ip | IP 주소 | 서버 IP 주소 (IPv4 또는 IPv6). |
| server.mac | dst\_mac | 문자열 | 서버 MAC 주소 |
| server.nat.ip | nat\_dst\_ip | IP 주소 | NAT 목적지 IP |
| server.nat.port | nat\_dst\_port | 32비트 정수 | NAT 목적지 포트 |
| server.packets | rcvd\_pkts | 64비트 정수 | 서버가 클라이언트로 전송한 패킷 수 |
| server.port | dst\_port | 32비트 정수 | 서버 포트 |
| server.registered\_domain | dst\_eld | 문자열 | 목적지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| server.subdomain | dst\_subdomain | 문자열 | 목적지 서브도메인 |
| server.top\_level\_domain | dst\_tld | 문자열 | 목적지 TLD |

### Source 필드

source 필드는 네트워크 교환/패킷의 발신자에 대한 세부 정보를 캡처합니다. 이러한 필드는 네트워크 이벤트, 패킷 또는 네트워크 트랜잭션의 세부 정보가 포함된 기타 이벤트에서 채워집니다.

source 필드는 일반적으로 destination 필드와 함께 채워집니다. source 및 destination 필드는 기본 요소이므로 이벤트에 네트워크 트랜잭션의 소스 및 대상 세부 정보가 포함된 경우 항상 채워져야 합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| source.address | src\_addr | 문자열 | 출발지 주소. IP 주소, 도메인 등 모든 형태의 문자열 |
| source.bytes | sent\_bytes | 64비트 정수 | 출발지에서 목적지로 전송한 바이트 수 |
| source.domain | src\_host | 문자열 | 출발지 도메인 이름 |
| source.ip | src\_ip | IP 주소 | 출발지 IP 주소 (IPv4 또는 IPv6). |
| source.mac | src\_mac | 문자열 | 출발지 MAC 주소 |
| source.nat.ip | nat\_src\_ip | IP 주소 | NAT 출발지 IP 주소 |
| source.nat.port | nat\_src\_port | 32비트 정수 | NAT 출발지 포트 |
| source.packets | sent\_pkts | 64비트 정수 | 출발지에서 목적지로 전송한 패킷 수 |
| source.port | src\_port | 32비트 정수 | 출발지 포트 |
| source.registered\_domain | src\_eld | 문자열 | 출발지 등록된 도메인 이름. 예를 들어, demo.acme.com이면 acme.com |
| source.subdomain | src\_subdomain | 문자열 | 출발지 서브도메인 |
| source.top\_level\_domain | src\_tld | 문자열 | 출발지 TLD |
| source.user.domain | src\_nt\_domain | 문자열 | 출발지 계정이 속한 액티브 디렉터리 또는 LDAP 도메인 이름. |
| source.user.email | mail\_from | 문자열 | 출발지 계정 이메일 |
| source.user.full\_name | src\_emp\_name | 문자열 | 출발지 사용자 성명 |
| source.user.hash | src\_user\_hash | 문자열 | 출발지 계정 익명화 필요 시 계정 해시 값 |
| source.user.id | src\_user\_id | 문자열 | 출발지 계정 식별자. 예: S-1-5-21-202424912787-2692429404-2351956786-1000 |
| source.user.name | src\_user | 문자열 | 출발지 로그인 이름 |
| source.user.roles | src\_user\_roles | 문자열 | 이벤트 발생 시점에 출발지 사용자가 보유한 역할 목록 |

### TLS 필드

TLS 연결과 관련된 필드. 이러한 필드는 TLS 프로토콜 자체에 초점을 맞추며 x.509 인증서 파일과 관련된 필드는 별도로 정의합니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| tls.cipher | tls\_cipher | 문자열 | 선택된 암호화 스위트. 예: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| tls.client.certificate | tls\_client\_cert | 문자열 | PEM 인코딩된 클라이언트 인증서 |
| tls.client.certificate\_chain | tls\_client\_cert\_chain | 리스트 | PEM 인코딩된 클라이언트 인증서 체인 |
| tls.client.hash.md5 | tls\_client\_cert\_md5 | 문자열 | 클라이언트 인증서 MD5 지문 |
| tls.client.hash.sha1 | tls\_client\_cert\_sha1 | 문자열 | 클라이언트 인증서 SHA1 지문 |
| tls.client.hash.sha256 | tls\_client\_cert\_sha256 | 문자열 | 클라이언트 인증서 SHA256 지문 |
| tls.client.issuer | tls\_client\_cert\_issuer | 문자열 | 클라이언트 인증서 발급자 |
| tls.client.ja3 | tls\_client\_ja3 | 문자열 | 클라이언트 SSL/TLS 핸드쉐이크에 대한 JA3 해시 |
| tls.client.not\_after | tls\_client\_not\_after | 날짜 | 클라이언트 인증서 유효기간 시작 일시 |
| tls.client.not\_before | tls\_client\_not\_before | 날짜 | 클라이언트 인증서 유효기간 만료 일시 |
| tls.client.server\_name | tls\_client\_sni | 문자열 | 클라이언트 인증서 SNI |
| tls.client.subject | tls\_client\_subject | 문자열 | 클라이언트 인증서 제목 |
| tls.client.supported\_ciphers | tls\_client\_supported\_ciphers | 문자열 | 클라이언트가 지원하는 암호화 스위트 목록 |
| tls.curve | tls\_curve | 문자열 | 커브 암호화 알고리즘. 예: secp256r1 |
| tls.established | tls\_established | 불리언 | TLS 협상 성공 여부 |
| tls.next\_protocol | tls\_next\_protocol | 문자열 | 다음 프로토콜 이름. 예: http/1.1 |
| tls.resumed | tls\_resumed | 불리언 | 기존 TLS 협상 조건으로 통신 재개 여부 |
| tls.server.certificate | tls\_server\_cert | 문자열 | PEM 인코딩된 서버 인증서 |
| tls.server.certificate\_chain | tls\_server\_cert\_chain | 리스트 | PEM 인코딩된 서버 인증서 체인 |
| tls.server.hash.md5 | tls\_server\_cert\_md5 | 문자열 | 서버 인증서 MD5 지문 |
| tls.server.hash.sha1 | tls\_server\_cert\_sha1 | 문자열 | 서버 인증서 SHA1 지문 |
| tls.server.hash.sha256 | tls\_server\_cert\_sha256 | 문자열 | 서버 인증서 SHA256 지문 |
| tls.server.issuer | tls\_server\_issuer | 문자열 | 서버 인증서 발급자. 예: CN=Example Root CA, OU=Infrastructure Team, DC=example, DC=com |
| tls.server.ja3s | tls\_server\_ja3s | 문자열 | 서버 SSL/TLS 핸드쉐이크에 대한 JA3S 해시. 예: 394441ab65754e2207b1e1b457b3641d |
| tls.server.not\_after | tls\_server\_not\_after | 날짜 | 서버 인증서 유효기간 시작 일시 |
| tls.server.not\_before | tls\_server\_not\_before | 날짜 | 서버 인증서 유효기간 만료 일시 |
| tls.server.subject | tls\_server\_subject | 문자열 | 서버 인증서 제목 예: CN=www.example.com, OU=Infrastructure Team, DC=example, DC=com |
| tls.version | tls\_ver | 문자열 | TLS 버전. 예: 1.2 |
| tls.version\_protocol | tls\_protocol | 문자열 | 정규화된 TLS 프로토콜 이름. 예: tls |

### User agent 필드

user\_agent 필드는 일반적으로 웹 서버 로그에 포함되어 있습니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| user\_agent.device.name | user\_agent\_device | 문자열 | 유저 에이전트에서 추출된 장비 이름. 예: iPhone |
| user\_agent.name | browser\_name | 문자열 | 유저 에이전트에서 추출된 브라우저 이름. 예: Safari |
| user\_agent.original | user\_agent | 문자열 | 유저 에이전트 원본 문자열 |
| user\_agent.version | browser\_ver | 문자열 | 유저 에이전트 버전. 예: 12.0 |

### VLAN 필드

VLAN 필드는 패킷의 802.1q 태그와 특정 패킷 또는 연결과 관련된 관찰자의 수신 및 송신 VLAN 연결을 식별하는데 사용됩니다.

#### 필드 변환

|  |  |  |  |
| --- | --- | --- | --- |
| 원본 필드 | 정규 필드 | 정규 타입 | ECS 필드 설명 |
| vlan.id | vlan\_id | 32비트 정수 | VLAN ID. 예: 10 |
| vlan.name | vlan\_name | 문자열 | VLAN 이름 예: outside |