### matchfeed

입력 레코드에서 지정된 필드의 값을 위협 인텔리전스 피드와 대조하여 필터링합니다.

#### 문법

matchfeed [invert=BOOL] [name=FEED\_ID] [type=TYPE] fields=FIELD\_LIST

'name=FEED\_ID'와 'type=TYPE'을 동시에 사용할 수 없습니다. 둘 중 하나만 사용하십시오.

필수 매개변수

**name=FEED\_ID**

fields로 지정된 필드 레코드와 대조할 위협 인텔리전스 피드 식별자(기본값: 없음). 식별자(FEED\_ID)는 다음 표를 참조하십시오.

|  |  |  |  |
| --- | --- | --- | --- |
| 이름 | 유형 | 이름 | 설명 |
| otx | IP 주소 | OTX 피드 | ISAC이 제공하는 OTX (Open Threat Exchange) IP 주소 피드 |
| tor | IP 주소 | TOR 프록시 | ISAC이 제공하는 Tor 네트워크의 EXIT 라우터 IP 주소 피드 |
| mdl\_domain | 도메인 | 악성 도메인 주소 목록 | ISAC이 제공하는 랜섬웨어 등 악성코드 도메인 주소 피드 |
| mdl\_ip | IP 주소 | 악성 IP 주소 목록 | ISAC이 제공하는 악성 IP 주소 피드 |
| abusech | 도메인 | abuse.ch | ISAC이 제공하는 abuse.ch 악성 도메인 주소 피드 |
| malc0de | MD5 | malc0de | ISAC이 제공하는 malc0de.com 악성코드 MD5 해시 피드 |
| logpresso\_cti\_ip | IP 주소 | 악성 IP 주소 목록 | 로그프레소 CTI 서비스에서 제공하는 악성 IP 주소 피드 |
| logpresso\_cti\_domain | 도메인 | 악성 도메인 주소 목록 | 로그프레소 CTI 서비스에서 제공하는 도메인 주소 피드 |
| logpresso\_cti\_url | URL | 악성 URL 목록 | 로그프레소 CTI 서비스에서 제공하는 URL 피드 |
| logpresso\_cti\_md5 | MD5 | 악성코드 MD5 해시 목록 | 로그프레소 CTI 서비스에서 제공하는 MD5 해시 피드 |
| logpresso\_cti\_sha1 | SHA1 | 악성코드 SHA1 해시 목록 | 로그프레소 CTI 서비스에서 제공하는 SHA1 해시 피드 |
| logpresso\_cti\_sha256 | SHA256 | 악성코드 SHA256 해시 목록 | 로그프레소 CTI 서비스에서 제공하는 SHA256 해시 피드 |

이 외에, 소나에 설치한 앱이 제공하는 피드를 사용할 수 있습니다. 앱이 제공하는 피드 식별자는 해당 앱의 문서를 참조하십시오.

**type=TYPE**

위협 인텔리전스 피드와 대조할 값의 유형(기본값: 없음). 지정할 수 있는 값은 domain, email, ip, md5, sha256, url 입니다. type 옵션을 사용하면 해당 유형 정보가 포함된 모든 위협 인텔리전스 피드와 fields로 지정된 필드 값을 대조합니다.

* domain: 유형이 도메인 주소인 모든 피드
* ip: 유형이 IP 주소인 모든 피드
* md5: 유형이 MD5 해시인 모든 피드
* sha1: 유형이 SHA1 해시인 모든 피드
* sha256: 유형이 SHA256 해시인 모든 피드
* url: 유형이 URL인 모든 피드

**fields=FIELD\_LIST**

위협 인텔리전스 피드와 값을 대조할 필드 목록. 공백문자 없이 구분자로 쉼표(,)를 사용합니다.

선택 매개변수

**invert=BOOL**

fields 옵션으로 지정한 값을 위협 인텔리전스 피드와 대조한 결과를 반환하는 방법(기본값: f)

* t: 대조 결과에 fields로 지정한 값이 포함되지 않은 레코드를 반환
* f: 대조 결과에 fields로 지정한 값이 포함된 레코드를 반환

#### 설명

피드 식별자와 명령을 실행한 다음 출력되는 필드 내용은 다음 표를 참조하십시오.

출력 필드

|  |  |  |
| --- | --- | --- |
| 필드 | 타입 | 설명 |
| feed\_name | 문자열 | 위협 인텔리전스 피드 식별자 |
| feed\_field | 문자열 | 위협 정보가 발견된 필드 이름 |
| feed\_invert | 불리언 | invert 옵션 값 |