### mpsearch

수천 개 이상의 키워드 패턴을 고속으로 한 번에 검색합니다. 서브쿼리에서 지정된 패턴이 검색 대상 필드에서 검출되면, **\_mp\_result** 필드에 검출된 모든 패턴 목록을 포함하여 출력합니다.

#### 문법

mpsearch [FIELD,...] [ SUBQUERY ]

필수 매개변수

**[FIELD,...]**

멀티 패턴을 검색할 대상 필드 목록. 쉼표(,)를 구분자로 사용합니다. 필드를 지정하지 않으면 모든 필드에 대해 검색을 수행합니다.

**[ SUBQUERY ]**

검색할 키워드 패턴의 목록을 조회하는 서브쿼리를 대괄호쌍([ ])으로 감싸서 입력

#### 설명

서브쿼리의 출력은 **expr**, **expr2**, **rule** 문자열 필드를 포함해야 합니다.

* **expr** (필수): 문자열을 불리언 표현식으로 조합하여 작성합니다. 스캔대상 필드의 문자열 값에서 해당되는 문자열을 고속으로 검출한 후, 표현식과 일치하는지 확인합니다.
* **expr2** (선택): **expr** 필드의 문자열 불리언 표현식이 참일 때, 다른 필드의 값을 이용해 추가 검색할 수 있는 기회를 선택적으로 제공합니다.
* **rule** (필수): 패턴 식별자 혹은 이름을 기입합니다.

패턴의 예시는 아래와 같습니다:

**패턴 예시**

|  |  |  |
| --- | --- | --- |
| expr (필수) | expr2 (선택) | rule (필수) |
| "addextendedproc" and "xp\_cmdshell" |  | xp\_cmdshell |
| "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" | zb now\_connect |

만약 xp\_cmdshell 패턴만 탐지되었다면, **\_mp\_result** 필드의 값은 아래와 같습니다:

[ { "expr": "\"addextendedproc\" and \"xp\_cmdshell\"", "rule": "xp\_cmdshell" } ]

#### 사용 예

외부 DB에서 패턴 목록을 로딩하여 signature 필드를 대상으로 멀티 패턴매칭

mpsearch signature [ dbquery RULE\_DB select rule, expr, expr2 from web\_rules ]