### matchsig

필드의 문자열 값이 지정된 패턴 그룹에 포함되는지 확인하고 결과를 출력합니다.

#### 문법

matchsig [invert=BOOL] [verify=BOOL] guid=SIG\_GUID field=TARGET\_FIELD

필수 매개변수

**guid=SIG\_GUID**

패턴 그룹 GUID 식별자

**field=TARGET\_FIELD**

대상 필드 이름. 대상 필드의 값은 문자열 타입이어야 하며, 그 외의 키 값은 검색 실패로 간주합니다.

선택 매개변수

**invert=BOOL**

검색 결과의 출력 형식(기본값: f)

* t: 대상 필드의 값이 패턴 그룹에 포함되어 있지 않으면 출력
* f: 대상 필드의 값이 패턴 그룹에 포함되어 있어 있으면 출력

**verify=BOOL**

쿼리 파싱 단계에서 패턴 그룹 개체의 유효성 검사 여부(기본값: t).

* t: 패턴 그룹 개체의 유효성을 검증
* f: 패턴 그룹 개체의 유효성을 검증하지 않음. 이 옵션은 시스템이 정책 동기화 단계에서 문법 오류를 내지 않도록 하기 위해 설정합니다.

#### 설명

패턴 그룹은 네트워크 침입탐지 장비처럼 수천 개 이상의 키워드를 동시에 테스트할 수 있도록 아호 코라식(Aho-Corasick) 알고리즘을 사용합니다. 먼저 입력 문자열에 대해 패턴 그룹에 속한 모든 키워드를 한 번에 매칭하고, 그 후에 키워드로 선별된 패턴들의 검증식을 순차적으로 실행하여 최종적으로 패턴과 일치하는 룰 이름을 출력합니다.

**패턴 예시**

|  |  |  |
| --- | --- | --- |
| expr (필수) | expr2 (선택) | rule (필수) |
| 키워드 패턴: 1차 고속 탐지 | 불린 표현식: 2차 필터링 | 패턴 이름 |
| "addextendedproc" and "xp\_cmdshell" |  | xp\_cmdshell |
| "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" | zb now\_connect |

예를 들어, 패턴 "REMOTE\_ADDR" and ("fputs" or "fwrite") 검증식 path == "lib.php" 룰 zb now connect 로 설정한 경우, 대상 필드 값에서 REMOTE\_ADDR 문자열과 fputs 혹은 fwirte 문자열이 동시에 검색되는지 확인하고, 그 후에 path 필드 값이 lib.php 문자열과 일치하는지 확인합니다.