### flowsearch

서브쿼리로 정의된 IP 네트워크 대역, 포트, 프로토콜 조건으로 구성된 플로우 규칙을 읽어들여 입력 레코드와 대조하고, 검색된 모든 플로우 식별자를 **\_flow** 필드에 배열로 출력합니다.

#### 문법

flowsearch [ SUBQUERY ]

필수 매개변수

**[ SUBQUERY ]**

플로우 규칙을 정의하는 서브쿼리를 대괄호쌍([ ])으로 감싸서 입력합니다.

#### 설명

플로우 규칙은 파일, 테이블, 원격 RDBMS 등 임의의 위치에서 읽어올 수 있으며, 필드 구성과 타입이 일치해야 유효한 규칙으로 인식합니다. 서브쿼리로 적용할 수 있는 플로우 규칙은 10,000개를 초과할 수 없습니다. 10,001번째 규칙부터는 무시합니다.

서브쿼리가 실패하면 **\_flowsearch\_error** 필드에 오류 원인을 출력합니다. flowsearch 명령문 뒤에 **\_flowsearch\_error** 필드 값이 존재하는지 검사하는 예외 처리문을 두면 의도하지 않은 오류 혹은 오동작을 방지할 수 있습니다.

입력 필드

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 이름 | 타입 | 필수 여부 | 설명 |
| src\_ip | IP 주소 | 필수 | 출발지 IP 주소 |
| src\_port | 정수 | 선택 (null 허용) | 출발지 포트 |
| dst\_ip | IP 주소 | 필수 | 목적지 IP 주소 |
| dst\_port | 정수 | 선택 (null 허용) | 목적지 포트 |
| protocol | 문자열 | 선택 (null 허용) | 프로토콜 문자열 |

입력 레코드의 필드가 타입이 일치하지 않거나 필수 필드가 누락된 경우에는, 플로우 규칙을 검사하지 않고 레코드를 원본 그대로 출력합니다.

플로우 규칙 필드

|  |  |  |  |
| --- | --- | --- | --- |
| 필드 이름 | 타입 | 필수 여부 | 설명 |
| src\_ip | IP 주소 | 필수 | 출발지 IP 주소 |
| src\_cidr | 정수 | 필수 | 출발지 넷마스크 (0-32 범위의 정수) |
| src\_port | 정수 | 선택 (null 허용) | 출발지 포트 번호 (0-65535 범위의 정수) |
| dst\_ip | IP 주소 | 필수 | 목적지 IP 주소 |
| dst\_cidr | 정수 | 필수 | 목적지 넷마스크 (0-32 범위의 정수) |
| dst\_port | 정수 | 선택 (null 허용) | 목적지 포트 번호 (0-65535 범위의 정수) |
| protocol | 문자열 | 선택 (null 허용) | 프로토콜 문자열 (TCP, UDP, ICMP 등) |
| flow | 임의 타입 | 필수 | 플로우 식별자 |

즉, flowsearch 커맨드에 레코드가 1개 입력될 때마다 입력된 5-튜플 값을 플로우 규칙과 대조하여, 일치하는 플로우 식별자를 \_flow 필드에 목록으로 출력합니다.

플로우 규칙의 src\_ip, dst\_ip와 src\_cidr, dst\_cidr 필드는 모두 필수 입력이지만, 규칙의 src\_ip가 0.0.0.0 이고 src\_cidr이 0인 경우 모든 출발지 IP 주소에 대해 참이 되므로, 출발지 혹은 목적지에 대해 모든 값을 허용하려면 규칙에 0.0.0.0/0을 설정하면 됩니다.

예를 들어 아래의 플로우 규칙에 대해, 입력 레코드가 src\_ip=106.75.11.63, src\_port=57776, dst\_ip=106.246.20.67, dst\_port=80, protocol=TCP 인 경우, flow2가 일치하므로 출력 레코드에는 \_flow=["flow2"] 필드가 추가됩니다.

**플로우 규칙 예시**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| src\_ip | src\_cidr | src\_port | dst\_ip | dst\_cidr | dst\_port | protocol | flow |
| 211.36.133.0 | 24 | null | 106.246.20.67 | 32 | 80 | TCP | flow1 |
| 106.75.11.0 | 24 | null | 106.246.20.67 | 32 | null | TCP | flow2 |

#### 사용 예

json "{}"| eval src\_ip=ip("106.75.11.63"), src\_port=57776| eval dst\_ip=ip("106.246.20.67"), dst\_port=80, protocol="TCP"| # Initiating the flowsearch command that defines the flow search rule| flowsearch [ union [ json "{}" | eval src\_ip=ip("211.36.133.0"), dst\_ip=ip("106.246.20.67"), flow="flow1" ] | union [ json "{}" | eval src\_ip=ip("106.75.11.0"), dst\_ip=ip("106.246.20.67"), flow="flow2" ] | eval src\_cidr=24, dst\_cidr=32]| fields src\_ip, src\_port, dst\_ip, dst\_port, protocol, \_flow