### flowsearch

サブクエリで定義されたIPサブネットグループ、ポート、プロトコル条件で構成されるフロールールを読み込み、入力レコードと照合し、検出されたすべてのフロー識別子を\*\*\_flow\*\*フィールドに配列として出力します。

#### 構文

flowsearch [ SUBQUERY ]

**[ SUBQUERY ]**

フロールールを定義するクエリ文を角括弧（[ ]）内に入力してください。

#### 説明

フロールールはファイル、テーブル、リモートRDBMSなど任意の場所から読み込むことができ、フィールド構成および型が一致している場合に有効なルールとして認識されます。サブクエリで適用できるフロールールは10,000件までであり、10,001件目以降のルールは無視されます。

サブクエリが失敗した場合、**\_flowsearch\_error**フィールドにエラー原因が出力されます。flowsearchコマンドの後に\*\*\_flowsearch\_error\*\*フィールドの値が存在するかを検査する例外処理文を追加することで、意図しないエラーや誤動作を防止できます。

入力フィールド

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド名 | 型 | 必須かどうか | 説明 |
| src\_ip | IPアドレス | 必須 | 送信元IPアドレス |
| src\_port | 整数 | 任意（null可） | 送信元ポート |
| dst\_ip | IPアドレス | 必須 | 宛先IPアドレス |
| dst\_port | 整数 | 任意（null可） | 宛先ポート |
| protocol | 文字列 | 任意（null可） | プロトコル文字列 |

入力レコードのフィールド型が一致しない場合や必須フィールドが欠落している場合は、フロールールを検査せず、レコードを元のまま出力します。

フロールールフィールド

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド名 | 型 | 必須かどうか | 説明 |
| src\_ip | IPアドレス | 必須 | 送信元IPアドレス |
| src\_cidr | 整数 | 必須 | 送信元ネットマスク（0～32の整数） |
| src\_port | 整数 | 任意（null可） | 送信元ポート番号（0～65535の整数） |
| dst\_ip | IPアドレス | 必須 | 宛先IPアドレス |
| dst\_cidr | 整数 | 必須 | 宛先ネットマスク（0～32の整数） |
| dst\_port | 整数 | 任意（null可） | 宛先ポート番号（0～65535の整数） |
| protocol | 文字列 | 任意（null可） | プロトコル文字列（TCP、UDP、ICMPなど） |
| flow | 任意の型 | 必須 | フロー識別子 |

つまり、flowsearchコマンドに1件のレコードが入力されるたびに、入力された5タプル値をフロールールと照合し、一致するフロー識別子を\_flowフィールドにリストとして出力します。

フロールールのsrc\_ip、dst\_ipおよびsrc\_cidr、dst\_cidrフィールドはすべて必須ですが、ルールのsrc\_ipが0.0.0.0かつsrc\_cidrが0の場合、すべての送信元IPアドレスに対して一致します。送信元または宛先に対してすべての値を許可したい場合は、ルールに0.0.0.0/0を設定してください。

例えば、下記のフロールールに対して、入力レコードがsrc\_ip=106.75.11.63, src\_port=57776, dst\_ip=106.246.20.67, dst\_port=80, protocol=TCPの場合、flow2が一致するため、出力レコードには\_flow=["flow2"]フィールドが追加されます。

**フロールール例**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

#### 使用例

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"| # フロー検索ルールを定義するflowsearchコマンドの実行| 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