### matchfeed

入力レコード内の指定フィールドの値を脅威インテリジェンスフィードと照合し、フィルタリングします。

#### 構文

matchfeed [invert=BOOL] [name=STR\_FEED] [type=TYPE] fields=FIELD\_LIST

「name=STR\_FEED」と「type=TYPE」は同時に指定できません。いずれか一方のみを使用してください。

必須パラメータ

**name=STR\_FEED**

fieldsで指定したフィールド値と照合する脅威インテリジェンスフィードの識別子（デフォルト：なし）。識別子（フィード識別子（STR\_FEED））は下表を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| 名前 | STR\_FEED | 種別 | 説明 |
| ログプレッソ・CTI IP | logpresso\_cti\_ip | IP | サイバー攻撃に関連する悪性IPアドレス情報 |
| ログプレッソ・CTIドメイン | logpresso\_cti\_domain | DOMAIN | マルウェア配布元、C&Cサーバ等の悪性ドメインアドレス情報 |
| ログプレッソ・CTI URL | logpresso\_cti\_url | URL | ログプレッソCTI URLインジケーター情報 |
| ログプレッソ・CTI MD5 | logpresso\_cti\_md5 | MD5 | ログプレッソCTI MD5ハッシュインジケーターフィード |
| ログプレッソ・CTI SHA1 | logpresso\_cti\_sha1 | SHA1 | ログプレッソCTI SHA1ハッシュインジケーターフィード |
| ログプレッソ・CTI SHA256 | logpresso\_cti\_sha256 | SHA256 | ログプレッソCTI SHA256ハッシュインジケーターフィード |

上記以外にも、ソナーにインストールされたアプリが提供するフィードを利用できます。アプリが提供するフィード識別子については、各アプリのドキュメントを参照してください。

**type=TYPE**

脅威インテリジェンスフィードと照合する値の種別（デフォルト：なし）。指定可能な値は domain、email、ip、md5、sha1、sha256、url です。typeオプションを指定すると、該当種別を持つすべての脅威インテリジェンスフィードと、fieldsで指定したフィールド値を照合します。

* domain: 種別がDOMAINのすべてのフィード
* email: 種別がEMAILのすべてのフィード
* ip: 種別がIPのすべてのフィード
* md5: 種別がMD5のすべてのフィード
* sha1: 種別がSHA1のすべてのフィード
* sha256: 種別がSHA256のすべてのフィード
* url: 種別がURLのすべてのフィード

標準搭載の脅威インテリジェンスフィードにはEMAIL種別のフィードは含まれていませんが、脅威インテリジェンスを提供するアプリによってはEMAIL種別のフィードが提供される場合があります。

**fields=FIELD\_LIST**

脅威インテリジェンスフィードと照合するフィールドリスト。区切り文字はカンマ（,）で、空白は含めません。

オプションパラメータ

**invert=BOOL**

fieldsオプションで指定した値を脅威インテリジェンスフィードと照合した結果の返却方法（デフォルト：f）

* t: 照合結果において、fieldsで指定した値が含まれていないレコードを返却
* f: 照合結果において、fieldsで指定した値が含まれているレコードを返却

#### 説明

フィード識別子およびコマンド実行後に出力されるフィールド内容は下表を参照してください。

出力フィールド

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| feed\_name | 文字列 | 脅威インテリジェンスフィード識別子 |
| feed\_field | 文字列 | 脅威情報が検出されたフィールド名 |
| feed\_invert | ブール値 | invertオプションの値 |