### matchfeed

Filters the input records using the threat intelligence feed from the Logpresso CTI.

#### Syntax

matchfeed name=FEED\_ID|type=TYPE fields=FIELD,... [invert=BOOL]

Required Parameter

**name=FEED\_ID**

The identifier of the threat intelligence feed to match against the field record specified by the fields option (default: none). The name=FEED\_ID and type=TYPE options cannot be used at the same time. Use either one.

See the following table for available identifiers. In addition, you can use the feeds provided by apps installed on Lopresso Sonar.

|  |  |  |
| --- | --- | --- |
| FEED\_ID | Type | Description |
| otx | ip | Real-time IP address reputation feed in the format of OTX (Open Threat Exchange) |
| tor | ip | Tor exit node IP address information feed |
| mdl\_domain | domain | Malicious domain name (e.g. C&C domain) feed |
| mdl\_ip | ip | Malicious domain name (e.g. C&C IP address) feed |
| abusech | domain | Malicious domain name (e.g. C&C domain) feed provided by abuse.ch |
| malc0de | md5 | Malware database provided by malc0de.com |

**type=TYPE**

The type of value to match against the threat intelligence feed. Valid values are domain, email, ip, md5, sha256, and url. The type option matches against all threat intelligence feeds with that type information. The name=FEED\_ID and type=TYPE options cannot be used at the same time. Use either one.

* domain: Domain name
* email: Email address
* ip: IP address
* md5: MD5 hash of the binary file
* sha256: SHA256 hash of the binary file
* url: URL

**fields=FIELD,...**

Fields to match values against threat intelligence feeds. Use comma (,) without any leading or trailing whitespaces as a separator.

Optional Parameter

**invert=BOOL**

Option to invert the result of matching the value specified by the fields option against the threat intelligence feed (default: f)

* t: Returns records that do not contain the value specified by fields in the matching result.
* f: Returns records that contain the value specified by fields in the matching result.

#### Description

Refer to the following table for the fields to be returned after executing the command and the feed identifiers.

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| feed\_name | String | Threat intelligence feed identifier |
| feed\_field | String | The name of the field where threat information was found |
| feed\_invert | Boolean | The value of the invert option |