

Runbook Transforming Squid Message

Date of Publish: 2019-3-18



Contents

Transform the Squid Message..... 3

Transform the Squid Message

You can customize your sensor data to provide more meaningful data. For example, you can choose to transform a url to provide the domain name of the outbound connection or the IP address. To do this, you need to add transformation information.

Procedure

1. In the Management module, click



(edit button) for your sensor.

The Management module displays the schema panel.

Squid

NAME *

Squid

No Matching Kafka Topic

PARSER TYPE *

Grok

GROK STATEMENT

SCHEMA

TRANSFORMATIONS	0
ENRICHMENTS	0
THREAT INTEL	0

THREAT TRIAGE

RULES	0
-------	---

SAVE

CANCEL

Advanced

- In the Schema box, click



(expand window button).

The Management module displays the Schema panel and populates it with message, field, and value information.

The Sample field, at the top of the panel, displays a parsed version of a sample message from the sensor. The Management module will test your transformations against this parsed message.

You can use the right and left arrow buttons in the Sample field to view the parsed version of each sample message available from the sensor.

You can apply transformations to an existing field or create a new field. Typically users choose to create and transform a new field, rather than transforming an existing field.

3. To add a new transformation, either click the

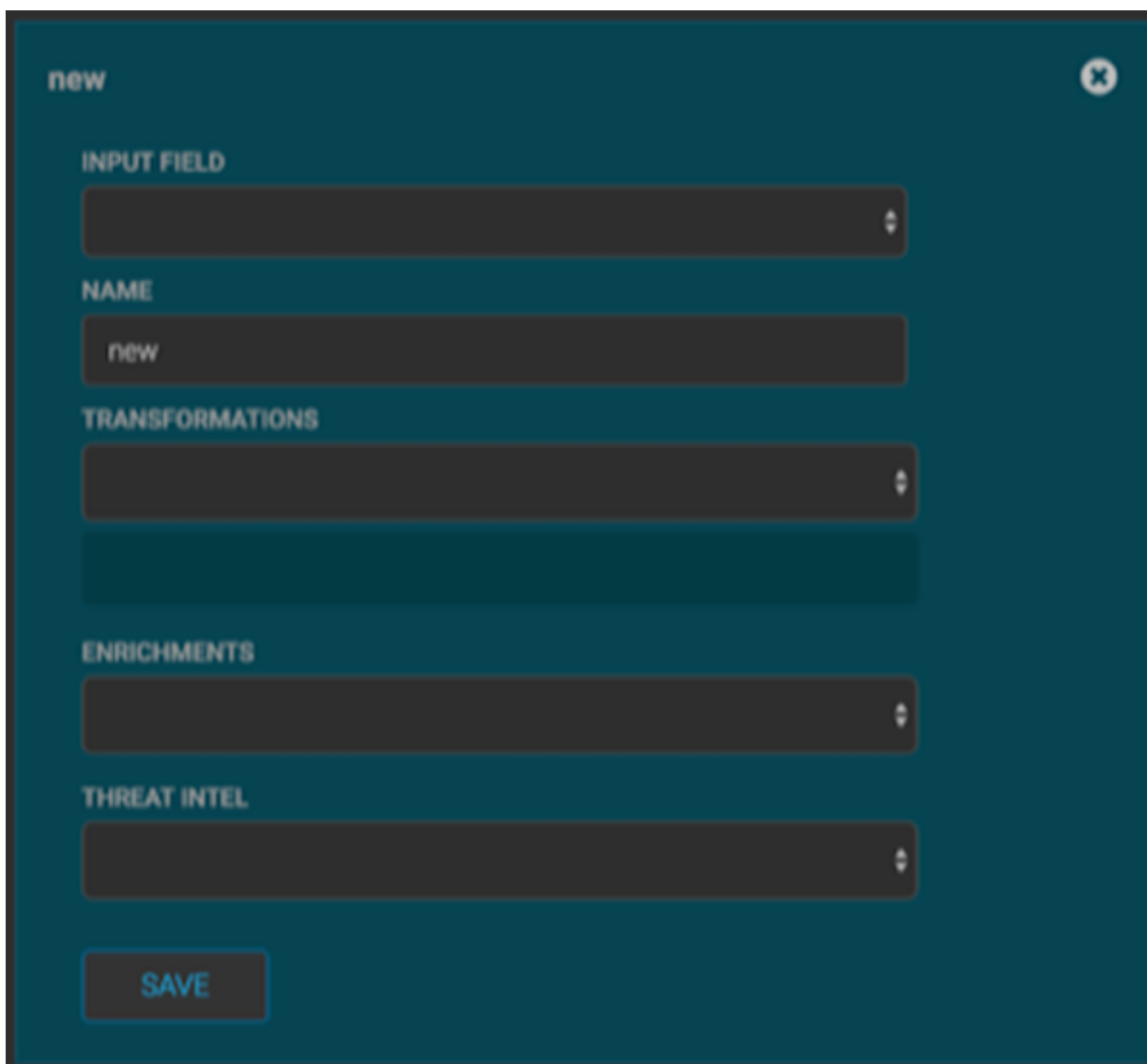


next to a field or click the



(plus sign) at the bottom of the **Schema** panel.

The module displays a new dialog box for your transformations.



The screenshot shows a configuration window titled "new" with a close button in the top right corner. The window contains several sections for configuring a transformation:

- INPUT FIELD**: A text input field.
- NAME**: A text input field containing the text "new".
- TRANSFORMATIONS**: A list of transformation functions. The first item is highlighted in blue, and a second, empty item is visible below it.
- ENRICHMENTS**: A text input field.
- THREAT INTEL**: A text input field.
- SAVE**: A button at the bottom left.

4. Choose the field you want to transform from the **INPUT FIELD** box, enter the name of the new field in the **NAME** field, and then choose a function with the appropriate parameters in the **TRANSFORMATIONS** box. You can apply more than transformation to the input field.

ip_dst_addr_copy

INPUT FIELD

ip_dst_addr

NAME

ip_dst_addr_copy

TRANSFORMATIONS

DOMAIN_REMOVE_SUBDOMAINS -

DOMAIN_REMOVE_TLD -

DOMAIN_REMOVE_TLD(DOMAIN_REMOVE_SUBDOMAINS(ip_dst_addr))

ENRICHMENTS

THREAT INTEL

SAVE

5. Click **SAVE** to save your additions.

The Management module populates the Transforms field with the number of transformations applied to the sensor. If you change your mind and want to remove a transformation, click "-" next to the field.

6. Click **SAVE** in the parser panel to save the transformation information.