

## Runbook Prioritizing Threat Intelligence

Date of publish: 2017-11-06



## Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

**Prioritizing Threat Intelligence Overview..... 4**

    Prerequisites..... 4

    Threat Triage Examples..... 4

    Perform Threat Triage..... 4

    View Triaged Alerts Using Kafka..... 7

    View Triaged Alerts Using the Metron Dashboard..... 7

## Prioritizing Threat Intelligence Overview

Not all threat intelligence indicators are equal. Some require immediate response, while others can be dealt with or investigated as time and availability permits. As a result you need to triage and rank threats by severity.

In Cloudera Cybersecurity Platform (CCP), you assign severity by associating possibly complex conditions with numeric scores. Then, for each message, you use a configurable aggregation function to evaluate the set of conditions and to aggregate the set of numbers for matching conditions. This aggregated score is added to the message in the `threat.triage.level` field.

### Prerequisites

Before you can prioritize a threat intelligence enrichment, you must ensure that the enrichment is working properly.

### Threat Triage Examples

Threat triage rules identify the conditions in the data source data flow and associate alert scores with those conditions.

Following are some examples of threat triage rules:

#### Rule 1

If a threat intelligence enrichment type is alerted, imagine that you want to receive an alert score of 5.

#### Rule 2

If the URL ends with neither `.com` nor `.net`, then imagine that you want to receive an alert score of 10.

### Perform Threat Triage

To create a threat triage rule configuration, you must first define your rules. These rules identify the conditions in the data source data flow and associate alert scores with those conditions.

#### Procedure

1.



Click the (edit button) for your sensor.

2.



In the Threat Triage field, click the icon (expand window).

The module displays the Threat Triage Rules panel.

Threat Triage Rules Panel

The screenshot displays two side-by-side configuration panels in a dark-themed interface.

**Left Panel: snort**

- NAME \***: A text input field containing "snort".
- Kafka Topic Exists, Emitting**: A green status message.
- PARSER TYPE \***: A dropdown menu showing "Snort".
- SCHEMA**: A table showing the number of items for each category:

Category	Count
TRANSFORMATIONS	1
ENRICHMENTS	4
THREAT INTEL	2
- THREAT TRIAGE**: A section with a "RULES 1" button.
- Buttons**: "SAVE", "CANCEL", and "Advanced" (text link).

**Right Panel: Threat Triage Rules**

- AGGREGATOR**: A dropdown menu showing "MAX".
- Rules**: Three buttons with colored dots and numbers: a red dot with "0", a yellow dot with "0", and a green dot with "1".
- Sort by**: A dropdown menu showing "Highest Score".
- Rule List**: A single rule entry with a yellow bar, the number "10", and the text "not(IN\_SUBNET(ip\_dst\_add...)".
- + Button**: A large blue button with a white plus sign to add a new rule.

- Click the **+** button to add a rule.  
The module displays the **Edit Rule** panel.  
Edit Rule Panel

4. Assign a name to the new rule by entering the name in the NAME field.
5. In the Text field, enter the syntax for the new rule.

```
Exists(IsAlert)
```

6. Use the **SCORE ADJUSTMENT** slider to choose the threat score for the rule.
7. Click **SAVE** to save the new rule.  
The new rule is listed in the Threat Triage Rules panel.
8. Choose how you want to aggregate your rules by choosing a value from the Aggregator menu.  
You can choose between:

#### MAX

The maximum of all of the associated values for matching queries.

#### MIN

The minimum of all of the associated values for matching queries.

#### MEAN

the mean of all of the associated values for matching queries.

#### POSITIVE\_MEAN

The mean of the positive associated values for the matching queries.

9. You can use the **Rules** section and the **Sort by** pull down menu below the **Rules** section to filter how threat triages display.  
For example, to display only high levels alerts, click the box containing the red indicator. To sort the high level alerts from highest to lowest, choose **Highest Score** from the **Sort by** pull down menu.
10. Click **SAVE** on the Sensor panel to save your changes.

## View Triage Alerts Using Kafka

You can view triaged alerts in the indexing topic in Kafka.

### Procedure

1. List the Kafka topics to find the threat triage alert panel:

```
/usr/hdp/current/kafka-broker/bin/kafka-topics.sh --zookeeper
$ZOOKEEPER_HOST:2181 --list
```

2. View the threat triage alert Kafka topic:

```
cd $METRON_HOME/bin/.stellar
THREAT_TRIAGE_PRINT(conf)
```

The topic should appear similar to the following:

```
> THREAT_TRIAGE_PRINT(conf)
#####
# Name                               # Comment # Triage Rule
#                               # Score # Reason
#
#####
# Abnormal DNS Port #               # source.type == "bro" and protocol == "dns"
# and ip_dst_port != 53 # 10        # FORMAT("Abnormal DNS Port: expected: 53,
# found: %s:%d", ip_dst_addr, ip_dst_port) #
#####
```

## View Triage Alerts Using the Metron Dashboard

You can view triaged alerts in the triaged alert panel in the CCP Metron dashboard.

The following figure shows you an example of a triaged alert panel in the Cloudera Cybersecurity Platform (CCP) Metron dashboard. For URLs from cnn.com, no threat alert is shown, so no triage level is set. Notice the lack of a threat.triage.level field:

Investigation Module Triage Alert Panel



Time	source_type	threat.triage.level	full_hostname	ip_src_addr	ip_dst_addr
June 29th 2016, 17:14:30.463	squid	5	www.ackthaka.com	127.0.0.1	198.50.236.7
June 29th 2016, 17:14:29.196	squid	5	www.ackthaka.com	127.0.0.1	198.50.236.7
June 29th 2016, 17:14:28.025	squid	5	www.ackthaka.com	127.0.0.1	198.50.236.7