Runbook Prioritizing Threat Intelligence

Date of Publish: 2018-10-15

http://docs.hortonworks.com

Contents

Prioritizing Threat Intelligence

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 Hortonworks Cybersecurity Platform (HCP), 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

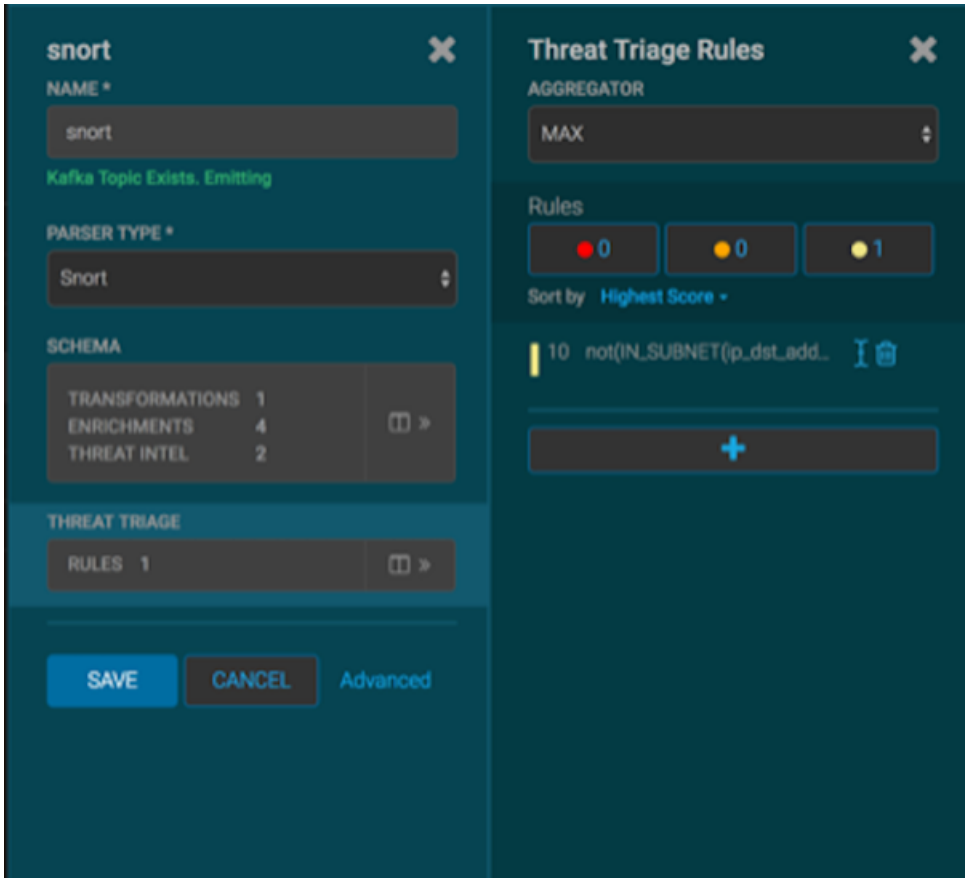
To create a threat triage rule configuration, you must first define your rules. These rules identify the conditions in the data source data flow and associate alert scores with those conditions.

Procedure

1. Click the  (edit button) for your sensor.
2. In the Threat Triage field, click the  icon (expand window).

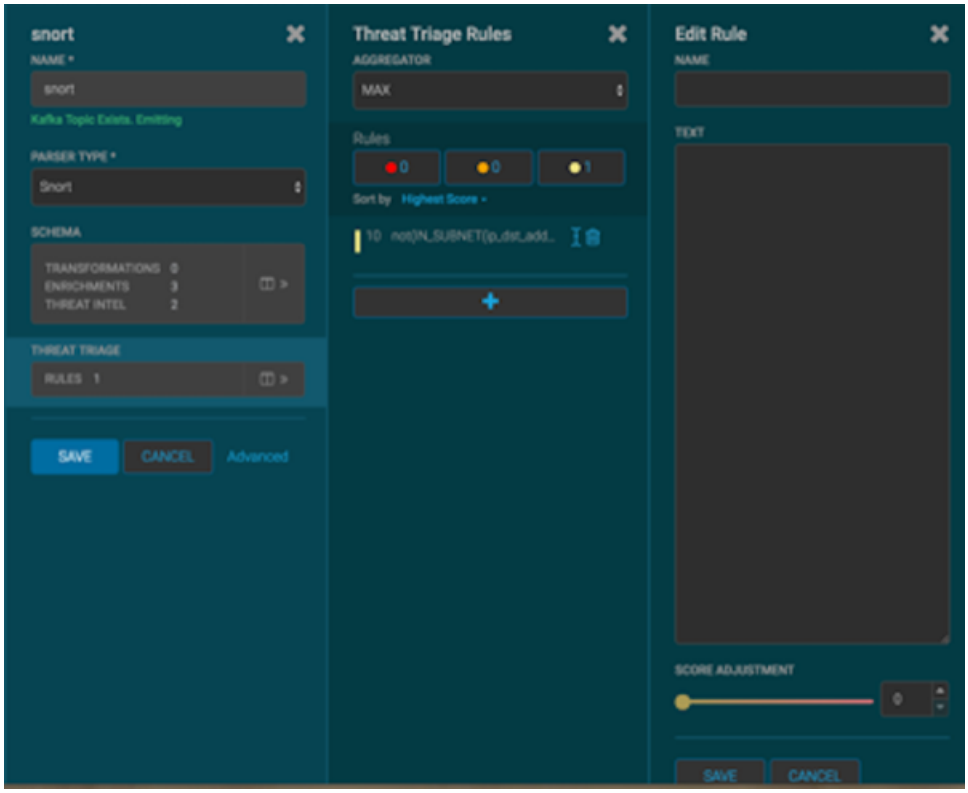
   The module displays the Threat Triage Rules panel.

   Threat Triage Rules Panel



3. 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 Triaged 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 Triaged Alerts Using the Metron Dashboard

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

The following figure shows you an example of a triaged alert panel in the Hortonworks Cybersecurity Platform (HCP) 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 Triaged Alert Panel