

HCP Enriching Telemetry Events 1

Introduction to Metron Dashboard

Date of Publish: 2018-10-15

<http://docs.hortonworks.com>

Contents

| | |
|--|----------|
| Introduction to Metron Dashboard..... | 3 |
| Functionality of Metron Dashboard..... | 3 |
| Metron Default Dashboard..... | 4 |
| Events..... | 5 |
| Enrichment..... | 5 |
| YAF..... | 6 |
| Snort..... | 6 |
| Web Request Header..... | 7 |
| DNS..... | 7 |

Introduction to Metron Dashboard

The Metron dashboard is a Kibana-based dashboard designed to identify, investigate, and analyze cybersecurity data. HCP supports Kibana 5.6.x. Kibana is an open source analytics and visualization platform.

Functionality of Metron Dashboard

The Metron dashboard displays all of the data on a single dashboard enabling you to filter through the irrelevant data and display just the information, alerts, and context for which you are looking.

The Metron dashboard has several advantages over conventional SIEM tools, including flexibility, and the single pane of glass approach that displays all of the data on the same screen, requiring no jumping from console to console to gather the information.

Dashboard-Snort Panel

Snort Overview

Snort is a Network Intrusion Detection System (NIDS) that is being used to generate alerts identifying known bad events. Snort relies on a fixed set of rules that act as signatures for identifying abnormal events.

Snort Alert Types

2
Alert Type(s)

Snort Top Alerts By Host

| Source | Destination | Count |
|-----------------|-----------------|-------|
| 192.168.138.158 | 62.75.195.236 | 12 |
| 192.168.138.158 | 95.163.121.204 | 5 |
| 192.168.138.158 | 72.34.49.86 | 4 |
| 192.168.138.158 | 204.152.254.221 | 1 |

Snort Alerts

| Time | msg | sig_id | ip_src_addr | ip_src_port | ip_dst_addr | ip_dst_port | protocol |
|---------------------------------|--|---------|-----------------|-------------|-----------------|-------------|----------|
| October 25th 2018, 12:01:37.000 | 'snort test alert' | 999,158 | 192.168.66.1 | 50,184 | 192.168.66.121 | 8,080 | TCP |
| October 25th 2018, 12:01:37.000 | 'snort test alert' | 999,158 | 192.168.66.1 | 50,184 | 192.168.66.121 | 8,080 | TCP |
| October 25th 2018, 12:01:37.000 | 'snort test alert' | 999,158 | 192.168.66.1 | 50,187 | 192.168.66.121 | 8,080 | TCP |
| October 25th 2018, 12:01:37.000 | 'snort test alert' | 999,158 | 62.75.195.236 | 80 | 192.168.138.158 | 49,186 | TCP |
| October 25th 2018, 12:01:37.000 | 'snort test alert' | 999,158 | 95.163.121.204 | 80 | 192.168.138.158 | 49,210 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 192.168.66.1 | 50,183 | 192.168.66.121 | 8,080 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 62.75.195.236 | 80 | 192.168.138.158 | 49,186 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 192.168.66.1 | 50,182 | 192.168.66.121 | 8,080 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 192.168.138.158 | 49,189 | 62.75.195.236 | 80 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 62.75.195.236 | 80 | 192.168.138.158 | 49,186 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 62.75.195.236 | 80 | 192.168.138.158 | 49,186 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 62.75.195.236 | 80 | 192.168.138.158 | 49,189 | TCP |
| October 25th 2018, 12:01:16.000 | 'snort test alert' | 999,158 | 72.34.49.86 | 80 | 192.168.138.158 | 49,204 | TCP |
| October 25th 2018, 12:01:16.000 | SERVER-WEBAPP Linksys router default username and password login attempt | 1,861 | 192.168.66.1 | 50,184 | 192.168.66.121 | 8,080 | TCP |

HCP supports two types of messages: metadata and alerts. By convention there should be one panel per metadata telemetry and one panel that is a "catch all" panel for alerts. The Snort panels are a good example of these two panel types. However, the Snort alerts panel only lists alerts from Snort because the default Metron dashboard contains only one data source that produces alerts.

When HCP parses the telemetry data on ingest, it extracts and normalizes different parts of the message into a standard Metron JSON. Standardizing and normalizing field names and format allows HCP to search different telemetry messages with a single query.

The first telemetry type that HCP supports is metadata messages. Metadata messages are parsed enriched messages in the JSON format.

The second telemetry type that HCP supports is alerts telemetries. Alerts telemetries come from IDS sensors like Snort or mixed telemetries like application logs that contain some metadata and some alert messages. While it is possible to set up a new panel for each alert telemetry, it is more desirable to set up a single panel that contains all of the alerts. This guarantees that the query will pull in alerts from multiple telemetries (even mixed mode telemetries that have some metadata and some alerts associated with them). You can then set up a detailed table containing only the alerts. To set telemetry as alert you need to set `is_alert = true`. This is already set up for HCP under the "Alerts" table.

The fields displayed for each alerts table can be customized. Ideally you want the fields of most importance (as well as the standard fields that telemetries are correlated on) to be displayed.

The following table contains a description of each of the Kibana components in the Metron dashboard.

| | |
|---------------------------------|---|
| Area Chart Panel | You can use the area chart panel for stacked timelines for which you want to see the total. |
| Data Table Panel | Use the data table panel to provide a detail breakdown, in tabular format, of the results of a composed aggregation. You can generate a data table from many other charts by clicking the grey bar at the bottom of the chart. |
| Detailed Message Panel | A detailed message panel displays the raw data from your search query. |
| Document Table | When you submit a search query, the 500 most recent documents that match the query are listed in the Documents table which is displayed in the center of the Discover window. |
| Field List | A list of all of the fields associated with a selected index pattern. This list is displayed on the left side of the Discover window. |
| Line Chart Panel | Use the line chart when you want to display high density time series. This chart is useful for comparing one series with another. |
| Mark Down Widget Panel | You can use the mark down widget panel to provide explanations or instructions for the dashboard. |
| Metric Panel | You can use a metric panel to display a single large number such as the number of hits or the average of a numeric field. |
| Pie Chart Panel | A pie chart is a circular statistical graphic that is ideal for displaying the parts of some whole. |
| Tile Map Panel | The tile map panel type displays a map populated with your search results. This panel type requires an Elasticsearch <code>geo_point</code> field that is mapped as <code>type:geo_point</code> with latitude and longitude coordinates. |
| Vertical Bar Chart Panel | You can use the vertical bar chart panel to display histograms. Histogram panels represent ingest rates for each individual telemetry. By convention, you should set up one for each type. |

Metron Default Dashboard

The default telemetry data sources installed with HCP help highlight the useful components available in Kibana 5.6.x. The default Metron dashboard serves as a starting point for you to build your own customized dashboards. During

installation, HCP sets up several telemetry data sources bundled with the platform and creates panels to display the associated data.

Events

The first panel in the dashboard highlights the variety of events being consumed by HCP. It shows the total number of events received, the variety of those events, and a histogram showing when the events were received.

Events



Enrichment

The next set of dashboard panels shows how HCP can be used to perform real-time enrichment of telemetry data. All of the IPv4 data received by HCP was cross-referenced against a geo-ip database. These locations were then used to build this set of dashboard components.

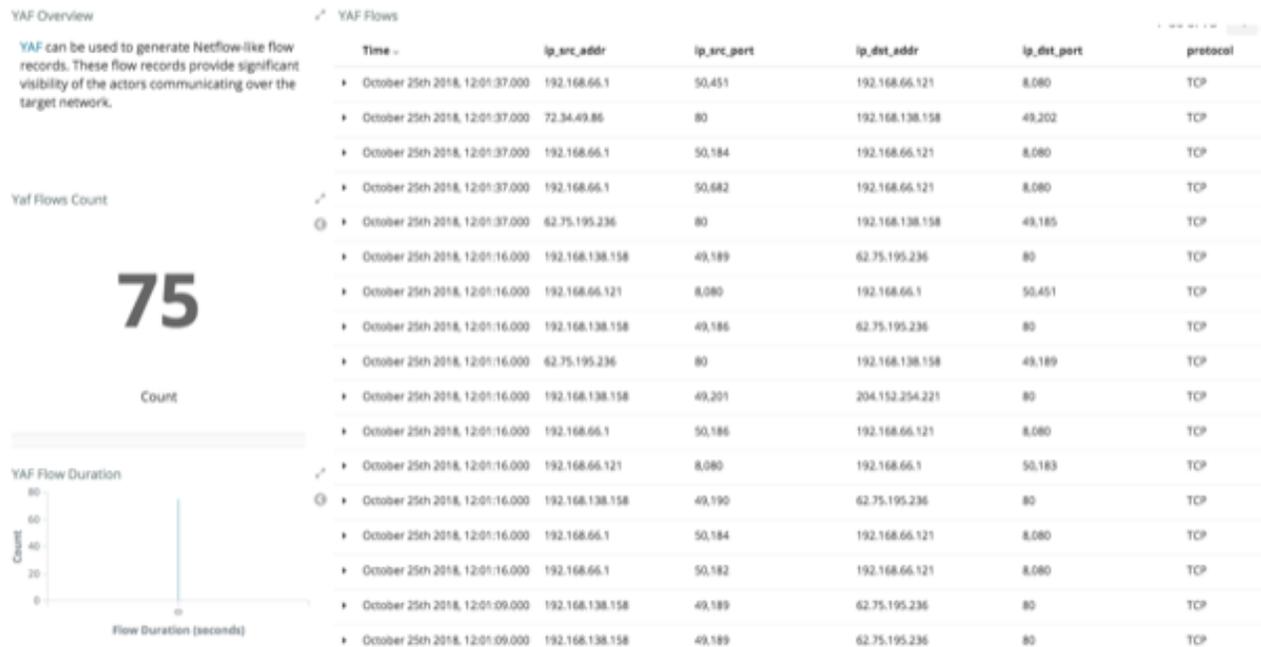
Enrichment



YAF

As part of the default sensor suite, YAF is used to generate flow records. These flow records provide significant visibility into which actors are communicating over the target network. A table panel displays the raw details of each flow record. A histogram of the duration of each flow illustrates that while most flows are relatively short-lived there are a few that are much longer in this example. Creating an index template that defined this field as numeric was required to generate the histogram.

YAF



Snort

Snort is a Network Intrusion Detection System (NIDS) that is being used to generate alerts identifying known bad events. Snort relies on a fixed set of rules that act as signatures for identifying abnormal events. Along with displaying the relevant details of each alert, the panel shows that there is only a single unique alert type; a test rule that creates a Snort alert on every network packet. Another table was created to show source/destination pairs that generated the most Snort alerts.

Dashboard-Snort Panel

DNS Requests Overview

Bro is extracting DNS requests and responses being made over the network. Understanding who is making those requests, the frequency, and types can provide a deep understanding of the actors present on the network.

DNS Requests

20

Count

DNS Requests

1-20 of 20

| Time | query | qtype_name | answers | ip_src_addr | ip_dst_addr |
|---------------------------------|--|------------|-----------------|-----------------|---------------|
| October 25th 2018, 12:01:37.120 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:01:16.975 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:01:09.979 | r03af42_c3008e_xd7h_80f_a99_x7f05a5e_u68f6i_e8mf6grf7g0_groupprograms.in | A | 62.75.195.236 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:01:09.081 | utbd7_3c147e_u805a4_w07c918_c07f1_b80w_r05a9_e8mf6grf7g0_groupprograms.in | A | 62.75.195.236 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:58.775 | vsf72g_g90e1h_b8_642b63u_j8f5a2_x33e_37_p429kcc_e8mf6grf7g0_groupprograms.in | A | 62.75.195.236 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:58.589 | comarkaaacounty.com | A | 72.34.49.86 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:58.489 | 7oqrsnzwmm6db7y.gigapaysun.com | A | 95.163.121.204 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:58.363 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:43.098 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:35.836 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:35.343 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:35.189 | runlive.us | A | 204.152.254.221 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:35.084 | vsf72g_g90e1h_b8_642b63u_j8f5a2_x33e_37_p429kcc_e8mf6grf7g0_groupprograms.in | A | 62.75.195.236 | 192.168.138.158 | 192.168.138.2 |
| October 25th 2018, 12:00:27.995 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:27.749 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |
| October 25th 2018, 12:00:27.376 | ._googlecast._tcp.local | PTR | - | 192.168.66.1 | 234.0.0.251 |