HCP Enriching Telemetry Events 1

# **Introduction to Metron Dashboard**

Date of Publish: 2018-12-21



https://docs.hortonworks.com/

# Contents

Introduction to Metron Dashboard	
Functionality of Metron Dashboard	
Metron Default Dashboard	4
Events	5
Enrichment	
YAF	
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 4.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	×	Sn	ort Alerts										
Snort is a Network Intrusion Detection System													
(NIDS) that is being used to generate alerts identifying known bad events. Snort relies on a			Time -	msg	sig_id	ip_src_addr	ip_src_pert	ip_dst_addr	ip_dst_port	protocol			
fixed set of rules that act as signatures for identifying abnormal events.		٠	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			
and you and the rest.		,	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 aliert'	999,158	192.168.66.1	50,187	192.168.66.121	8,080	TCP			
Snort Alert Types	0	,	October 25th 2018, 12:01:37.000	'snort test alert'	999,158	62.75.195.236	80	192.168.138.158	49,186	TCP			
		٠	October 25th 2018, 12:01:37.000	'snort test alert'	999,158	95.163.121.204	80	192.168.138.158	49,210	TCP			
2		٠	October 25th 2018, 12:01:16:000	'snort test aliert'	999,158	192.168.66.1	50,183	192.168.66.121	8,080	TCP			
<b>_</b>		,	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			
Alert Type(s)						•	October 25th 2018, 12:01:16:000	'snort test aliert'	999,158	192.168.138.158	49,189	62.75.195.236	80
Sec. (page		,	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			
Snort Top Alerts By Host Source Destination Count Count	í	•	October 25th 2018, 12:01:16:000	'snort test alert'	999,158	62.75.195.236	80	192.168.138.158	49,189	TCP			
192.168.138.158 62.75.195.236 12	1	,	October 25th 2018, 12:01:16.000	'snort test alert'	999,158	72.34.49.86	80	192.168.138.158	49,204	TCP			
192.168.138.158 95.163.121.204 5	1	,	October 25th 2018, 12:01:16:000	SERVER-WEBAPP	1,861	192.168.66.1	50.184	192.168.66.121	8.080	TCP			
192.168.138.158 72.34.49.86 4			Linksys router default username										
192.168.138.158 204.152.254.221 1				and password									
				login attempt									

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 <b>area chart panel</b> for stacked timelines for which you want to see the total.
Data Table Panel	Use the <b>data table panel</b> 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 <b>detailed message panel</b> 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 <b>Documents</b> table which is displayed in the center of the <b>Discover</b> 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 <b>Discover</b> window.
Line Chart Panel	Use the <b>line chart</b> 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 <b>mark down widget panel</b> to provide explanations or instructions for the dashboard.
Metric Panel	You can use a <b>metric panel</b> to display a single large number such as the number of hits or the average of a numeric field.
Pie Chart Panel	A <b>pie chart</b> is a circular statistical graphic that is ideal for displaying the parts of some whole.
Tile Map Panel	The <b>tile map panel</b> type displays a map populated with your search results. This panel type requires an Elasticsearch geo_point field that is mapped as type:geo_point with latitude and longitude coordinates.
Vertical Bar Chart Panel	You can use the <b>vertical bar chart panel</b> 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**

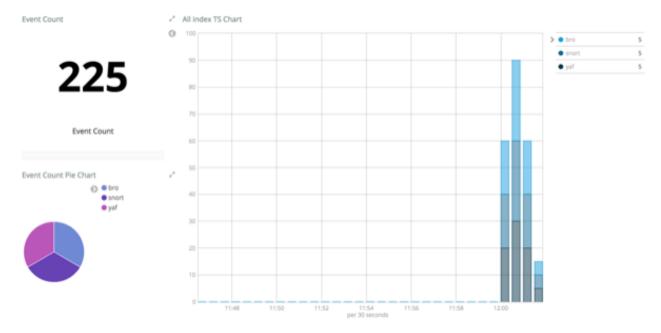
The default telemetry data sources installed with HCP help highlight the useful components available in Kibana 4. The default Metron dashboard serves as a starting point for you to build your own customized dashboards. During

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



5

### 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

YAF Overview	è	YA	F Flows					
YAF can be used to generate Netflow-like flow records. These flow records provide significant			Time -	lp_src_addr	ip_src_port	ip_dut_addr	ip_dst_port	protocol
visibility of the actors communicating over the		,	October 25th 2018, 12:01:37.000	192.168.66.1	50,451	192.168.66.121	8,080	TCP
target network.		,	October 25th 2018, 12:01:37.000	72.34.49.86	80	192.168.138.158	49,202	TCP
		,	October 25th 2018, 12:01:37.000	192.168.66.1	50,184	192.168.66.121	8,080	TCP
Yaf Flows Count	2	,	October 25th 2018, 12:01:37.000	192.168.66.1	50,682	192.168.66.121	8,080	TCP
	0	,	October 25th 2018, 12:01:37.000	62.75.195.236	80	192.168.138.158	49,185	TCP
		,	October 25th 2018, 12:01:16:000	192.168.138.158	49,189	62.75.195.236	80	TCP
75		,	October 25th 2018, 12:01:16:000	192.168.66.121	8,080	192.168.66.1	50,451	TCP
/3		,	October 25th 2018, 12:01:16.000	192.168.138.158	49,186	62.75.195.236	80	TCP
		,	October 25th 2018, 12:01:16:000	62.75.195.236	80	192.168.138.158	49,189	TCP
Count		,	October 25th 2018, 12:01:16:000	192.168.138.158	49,201	204.152.254.221	80	TCP
		,	October 25th 2018, 12:01:16:000	192.168.65.1	50,186	192.168.66.121	8,080	TCP
YAF Flow Duration	2	,	October 25th 2018, 12:01:16:000	192.168.66.121	8,080	192.168.66.1	50,183	TCP
80 -	0	,	October 25th 2018, 12:01:16.000	192.168.138.158	49,190	62.75.195.236	80	TCP
100 100 40		,	October 25th 2018, 12:01:16:000	192.168.66.1	50,184	192.168.66.121	8,080	TCP
20 -		,	October 25th 2018, 12:01:16:000	192.168.66.1	50,182	192.168.66.121	8.080	TCP
0		,	October 25th 2018, 12:01:09.000	192.168.138.158	49,189	62.75.195.236	80	TCP
Flow Duration (seconds)		,	October 25th 2018, 12:01:09.000	192.168.138.158	49,189	62.75.195.236	80	TCP

#### **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

Snort Overview	- 2	Sn	ort Alerts							
Snort is a Network Intrusion Detection Sys									1-50 of	75 <
(NIDS) that is being used to generate alerts identifying known bad events. Snort relies			Time	msg	sig_id	ip_src_addr	ip_src_port	ip_dst_addr	ip_dst_port	protocol
fixed set of rules that act as signatures for identifying abnormal events.		•	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
second of an an area to the		٠	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
Snort Alert Types	0	,	October 25th 2018, 12:01:37.000	'snort test alert'	999,158	62.75.195.236	80	192.168.138.158	49,186	TCP
	0	٠	October 25th 2018, 12:01:37,000	'snort test alert'	999,158	95.163.121.204	80	192.168.138.158	49,210	TCP
2			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
<b>_</b>		,	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
Alert Type(s)			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
Snort Top Alerts By Host Source Destination Cou	n Î	•	October 25th 2018, 12:01:16.000	'snort test alert'	999,158	62.75.195.236	80	192.168.138.158	49,189	TCP
192.168.138.158 62.75.195.236 12	-	,	October 25th 2018, 12:01:16.000	'snort test alert'	999,158	72.34.49.86	80	192.168.138.158	49,204	TCP
192.168.138.158 95.163.121.204 5	- 1	<ul> <li>October 25th 2018, 12:01:16:000</li> </ul>	SERVER-WEBAPP	1.861	192.168.66.1	50.184	192.168.66.121	8.080	TCP	
				Linksys router default username	- , , , , , , , , , , , , , , , , , , ,	1.000.1000.000.1		100.100.00.101		
				default username and password login attempt						
192.168.138.158 204.152.254.221 1										

#### Web Request Header

The Bro Network Security Monitor extracts application-level information from raw network packets. In this example, Bro is extracting HTTP and HTTPS requests being made over the network. The panels highlight the breakdown by request type, the total number of web requests, and raw details from each web request.

#### Dashboard-Bro Panel

W	eb Request Header Overview	23	Web Requests				
The Bro Network Security Monitor is extracting applicati level information from raw network packets. In this			Time -	method	heat	1-50 i	
	xample, Bro is extracting HTTP(S) requests being made ver the network.		October 25th 2018, 12:01:37:830	GET	ip-addr.es	1	
			October 25th 2018, 12/01/37,659	GET	node1	/www.industers/metron_dustermequests/to-endlapage_ster104/felds-fequests8_r168s168584696	http://node118 080/
W	th Requests	0	October 25th 2018, 12:01:37.628	GET	7oqnonoww nm6ab7y.gig apaysun.co an	/picture.php?k=11iqm/g&b312a994c3eaa4014608b222046c7964	http://?oqnanz www.milati?y.gi gapaytun.com /11iQm/g
			October 25th 2018, 12:01:07:501	POST	runiove.us	Anp-content/themes/twenty/fiteervlring5.php?u=mlym/?1rapdak	
	55		0006472092018,1201.16334	GET	node1	аран Подавалитела, была которонета? Ведан Банка Сопронения и на полно сопронения и полно сопронения и полно сопронения и полно сопронения и полно вак сопи сопронения и полно сопронения и полно сопронения сопронения и полно сопронения и полно сопронения и вак сопи сопронения и полно сопронения и по сопи сопронения и полно сопро Полно сопронения и полно сопрон	http://modef18 0807
	Count	1	October 25th 2018, 12:01:16.836	GET	node/1	$lapirel is lastern investors, strater in equests 7 s-end k page, size + 18 dividue-lasquests k_s + 168 + 1$	http://nodef18 080/
Web Requer	ob Request Type O # Git # POST	/	October 259-2018, 12:01.06.712	GET	x8667.3c14 76.x806a4.w 078919.x60 1.b80w.r0faf 9.e8mfbdgef 7g0.grouppr params.in	1	http://velf72g. g90e1h.b6.642 b65u.j985e3.v 33e.37.pe209c c.e8mfadgr77g 6.groupprogra ms.iv/?
			October 25th 2018, 12:01:16.605	GIT	nodw1	lapik/idustenimetror_dusteriomponents) hata_tangoverst/katakiakatakiakataki naki_tangoverst/katakiakatakiakatakiakataki naki_tangoverst/katakiakatakiakatakiakatakiakatakiakatakiakatakiakatakiakatakiakatakiakatakiakataki namohata_tomponentsikatakiakatakitakiakatakiakataki hatakitakiaka	http://hode118 080/

#### DNS

Bro extracts 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.

Dashboard-DNS Panel

192.168.66.1

192.168.66.1

234.0.0.251

224.0.0.251

DNS Requests Overview DNS Requests 1-20 of 20 < > 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. Time qtype,name ig.arc.addr ip.det.addr query answers October 25th 2018, 12:01:37.120 \_googlecast, ptp.local PTR 192.168.66.1 234.0.0.251 October 25th 2018, 12:01:16:975 \_googlecant\_top.local PTR 192.168.66.1 234.0.0.251 October 25th 2018, 12:01:05:979 r03aht2.c3008e.xtSTh 30f.a393.h795fa5eu.xb8hti.e8mfotgr17g5.grouppingnams.in 62.75.195.236 192.168.138.158 192,168,138,2 А. DNS Requests October 25th 2018, 12:01:08:081 ubb67.3c147o.u806a4.w07d918.o5f.f1.b80ev/0fa99.w8mfodgr7fg0.groupprograms.in 62.75.195.236 192108138158 192,168,138,2 A 0 October 25th 2018, 12:00:58.775 vid72g.g90e1h.38.642b63u (385a2 x33e.37.pa26bcx.e8mfbdgrf7g0.groupprograms.in 62.75.195.236 192.168.138.158 192,168,138,2 ..... October 25th 2018, 12:00:58,583 comarkaecurity.com . 72.34.49.86 192108138158 192,168,138,2 20 October 25th 2018, 12:00:58.469 Topronzwwnm6zb7y.gigapaysun.com А. 95.163.121.204 192.168.138.158 192,168,138,2 October 25th 2018, 12:00:58.363 \_googlecast\_top.local PTR 192.168.66.1 234.0.0.251 PTR October 25th 2018, 12:00:43.098 \_groglecast\_tcp.local 192.168.66.1 234.0.0.251 Count October 25th 2018, 12:00:35.836 \_googlecast, 3tp.local PTR 192.168.66.1 234.0.0.251 October 25th 2018, 12:00:35.343 \_grog/ecant\_tcp.local PTR 192.168.66.1 234.0.0.251 October 25th 2018, 12:00:35.169 numieve.us .... 204.152.254.221 192.168.138.158 192.168.138.2 October 25th 2018, 12:00:35:084 vs872g.g90e1h.b8.642b63u.j985a2x33e.37.pa200xz.e8mfzdgr77g0.groupprogram A 62.75.195.236 192.168.138.158 192,168,138,2 October 25th 2018, 12:00:27.995 \_googlecast, 3tp. local PTR 192.168.66.1 224.0.0.251

PTR

PTR

October 25th 2018, 12:08:27.749 \_googlecast, tcp.local

October 25th 2018, 12:00:27:376 \_grouplecast, \_tcp.local

8