CCP Enriching Telemetry Events 2.0.1

Introduction to Metron Dashboard

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

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

Introduction to Metron Dashboard

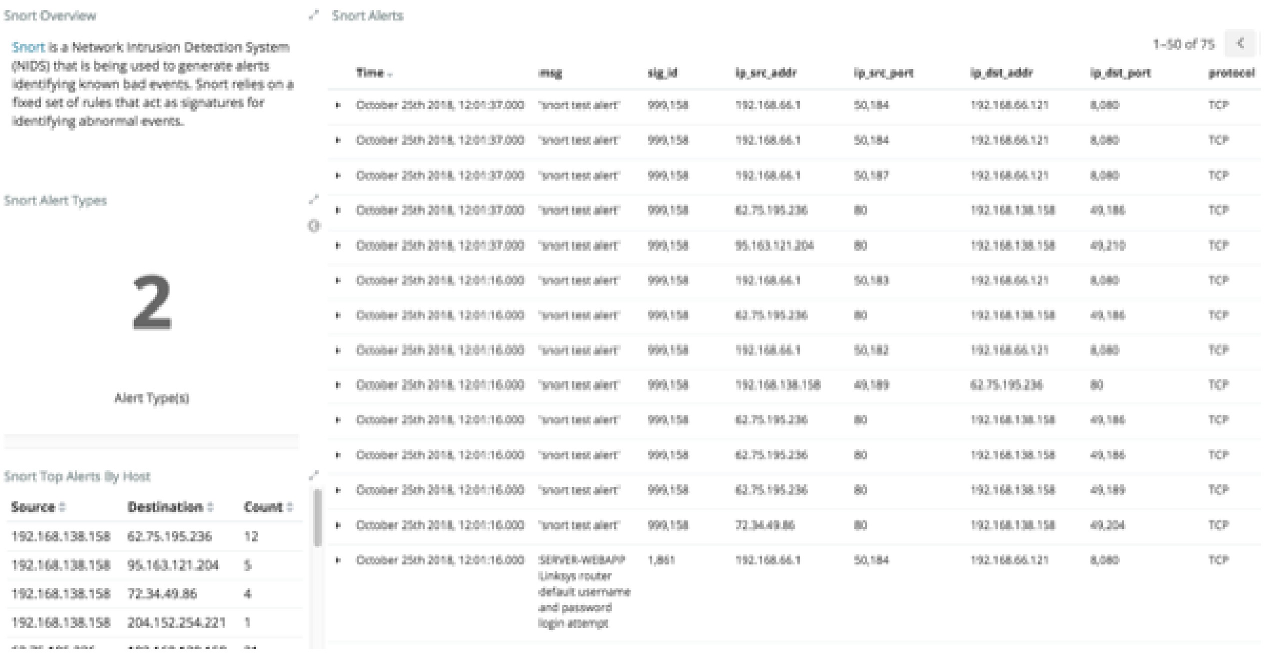
The Metron dashboard is a Kibana-based dashboard designed to identify, investigate, and analyze cybersecurity data. Cloudera Cybersecurity Platform (CCP) supports Kibana 4.x. Kibana is an open source analytics and visualization platform.

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

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

1–50 of 75

	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

CCP 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 CCP 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 CCP to search different telemetry messages with a single query.

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

The second telemetry type that CCP 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 CCP 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 geo_point field that is mapped as type:geo_point 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.

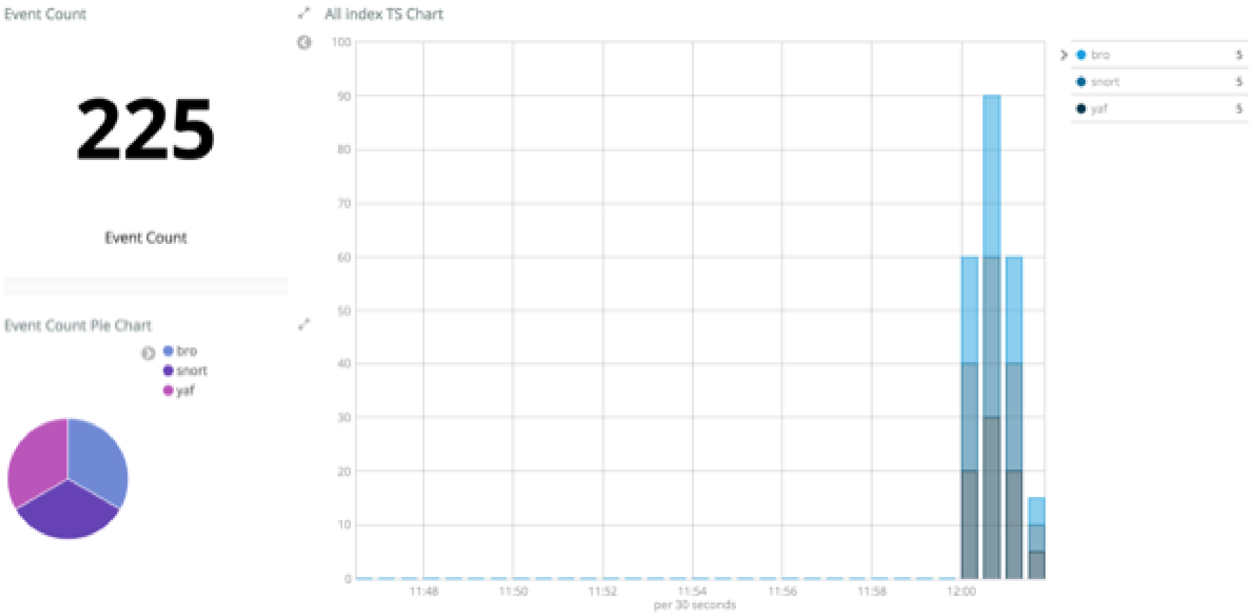
Metron Default Dashboard

The default telemetry data sources installed with Cloudera Cybersecurity Platform (CCP) 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, CCP 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 CCP. It shows the total number of events received, the variety of those events, and a histogram showing when the events were received.

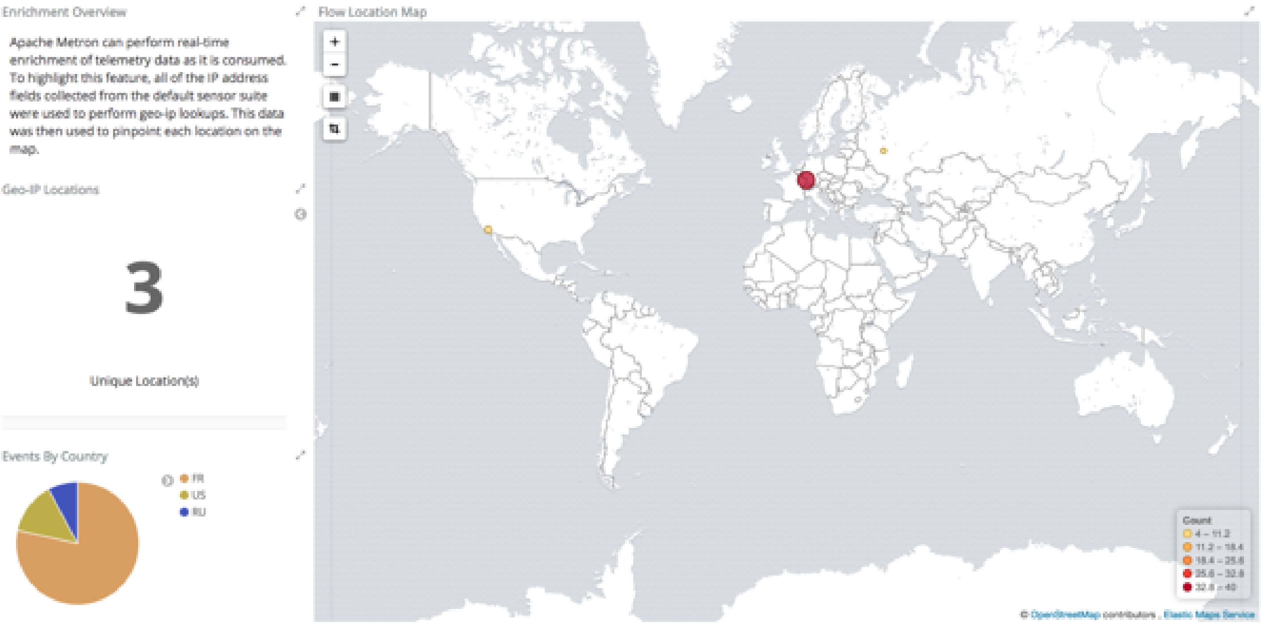
Events



Enrichment

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

Enrichment



Enrichment Overview

Apache Metron can perform real-time enrichment of telemetry data as it is consumed. To highlight this feature, all of the IP address fields collected from the default sensor suite were used to perform geo-ip lookups. This data was then used to pinpoint each location on the map.

Geo-IP Locations

3

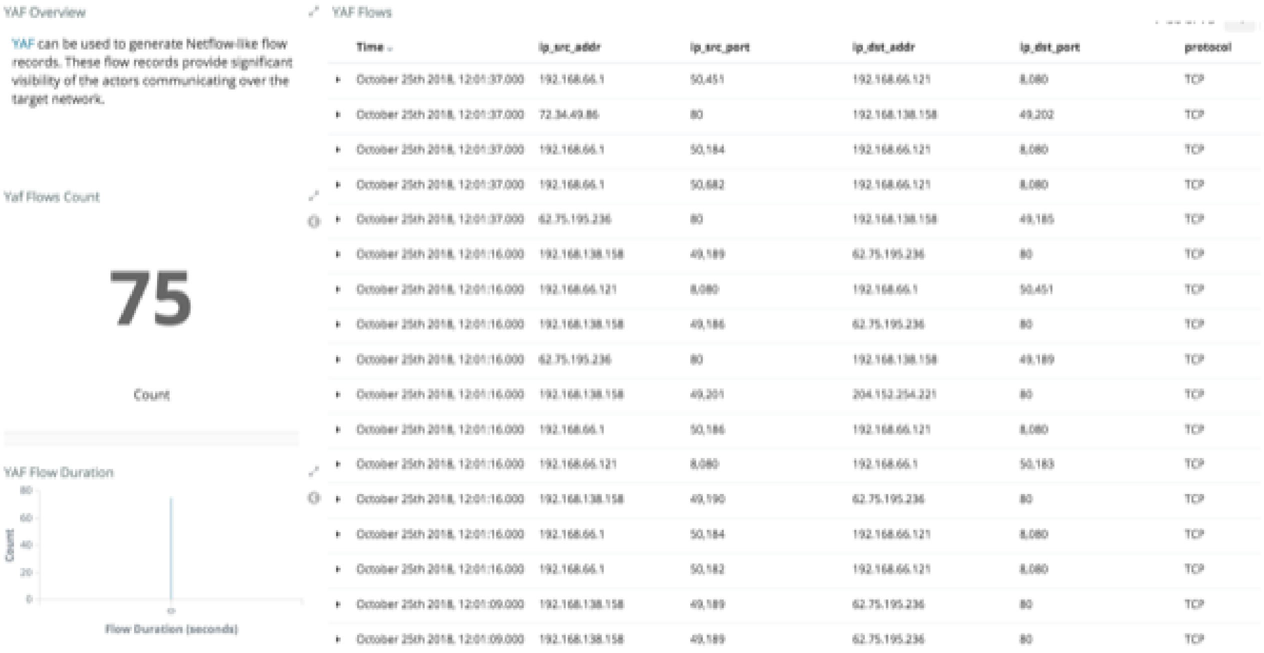
Unique Location(s)

Events By Country

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

YAF can be used to generate Netflow-like flow records. These flow records provide significant visibility of the actors communicating over the target network.

Yaf Flows Count

75

Count

YAF Flow Duration

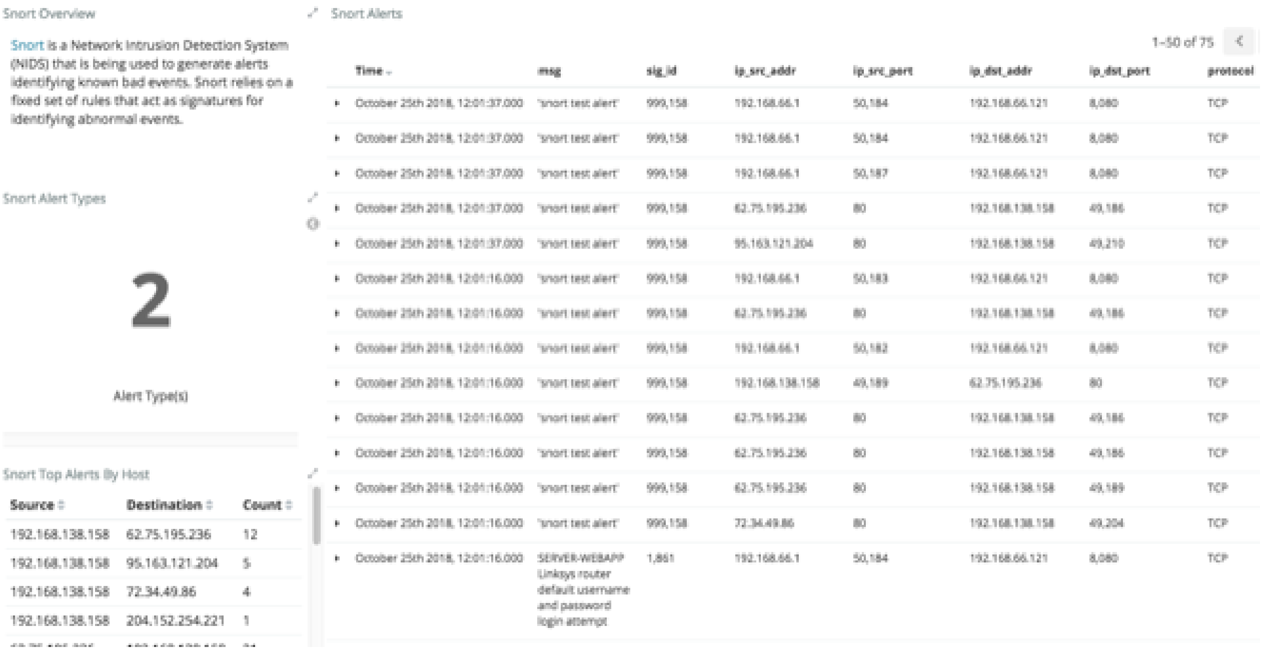
YAF Flows

Time	ip_src_addr	ip_src_port	ip_dst_addr	ip_dst_port	protocol
October 25th 2018, 12:01:37.000	192.168.66.1	50,451	192.168.66.121	8,080	TCP
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
October 25th 2018, 12:01:37.000	192.168.66.1	50,682	192.168.66.121	8,080	TCP
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
October 25th 2018, 12:01:16.000	192.168.66.121	8,080	192.168.66.1	50,451	TCP
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
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	192.168.66.1	50,186	192.168.66.121	8,080	TCP
October 25th 2018, 12:01:16.000	192.168.66.121	8,080	192.168.66.1	50,183	TCP
October 25th 2018, 12:01:16.000	192.168.138.158	49,190	62.75.195.236	80	TCP
October 25th 2018, 12:01:16.000	192.168.66.1	50,184	192.168.66.121	8,080	TCP
October 25th 2018, 12:01:16.000	192.168.66.1	50,182	192.168.66.121	8,080	TCP
October 25th 2018, 12:01:09.000	192.168.138.158	49,189	62.75.195.236	80	TCP
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

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
62.75.195.236	192.168.138.158	[illegible]

Snort Alerts

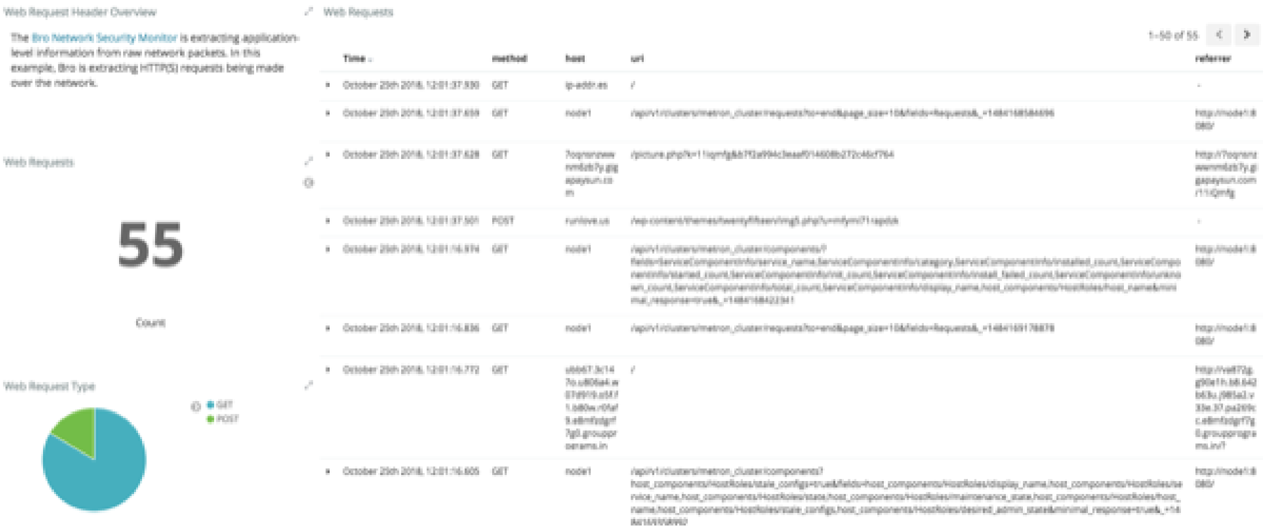
1–50 of 75

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

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



Web Request Header Overview

The Bro Network Security Monitor is extracting application-level information from raw network packets. In this example, Bro is extracting HTTP(S) requests being made over the network.

Web Requests

55

Count

Web Requests

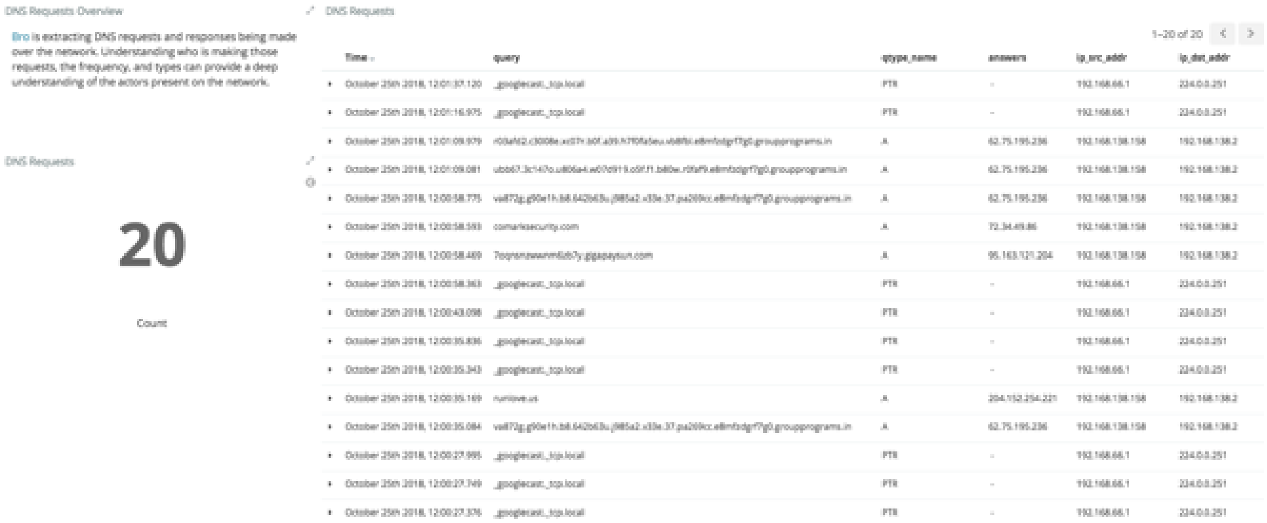
1–50 of 55

Time	method	host	uri	referrer
October 25th 2018, 12:01:37.930	GET	ip-addr.es	/	-
October 25th 2018, 12:01:37.659	GET	node1	/api/v1/clusters/metron_cluster/requests?to=end&page_size=10&fields=Requests&_=1484168584496	http://node1:8080/
October 25th 2018, 12:01:37.628	GET	7oqnsnzwwnm6zb7y.gigapaysun.com	/picture.php?k=11iqmfg&b7f2a994c3eaaf014608b272c46cf764	http://7oqnsnzwwnm6zb7y.gigapaysun.com/11iQmfg
October 25th 2018, 12:01:37.501	POST	runlove.us	/wp-content/themes/twentyfifteen/img5.php?u=mfymi71rapdzk	-
October 25th 2018, 12:01:16.974	GET	node1	/api/v1/clusters/metron_cluster/components?fields=ServiceComponentInfo/service_name,ServiceComponentInfo/category,ServiceComponentInfo/installed_count,ServiceComponentInfo/started_count,ServiceComponentInfo/init_count,ServiceComponentInfo/install_failed_count,ServiceComponentInfo/unknown_count,ServiceComponentInfo/total_count,ServiceComponentInfo/display_name,host_components/HostRoles/host_name&minimal_response=true&_=1484168422341	http://node1:8080/
October 25th 2018, 12:01:16.836	GET	node1	/api/v1/clusters/metron_cluster/requests?to=end&page_size=10&fields=Requests&_=1484169178878	http://node1:8080/
October 25th 2018, 12:01:16.772	GET	ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf5.e8mfzdgrf7g0.groupprograms.in	/	http://va872g.g90e1h.b8.642b63u.j985a2.v33w.37.pa269cc.e8mfzdgrf7g0.groupprograms.in/?
October 25th 2018, 12:01:16.605	GET	node1	/api/v1/clusters/metron_cluster/components?host_components/HostRoles/stale_configs=true&fields=host_components/HostRoles/display_name,host_components/HostRoles/service_name,host_components/HostRoles/state,host_components/HostRoles/maintenance_state,host_components/HostRoles/host_name,host_components/HostRoles/stale_configs,host_components/HostRoles/desired_admin_state&minimal_response=true&_=1484169158992	http://node1:8080/

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



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	224.0.0.251
October 25th 2018, 12:01:16.975	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251
October 25th 2018, 12:01:09.979	r00af62.c3008e.xc07r.b0f.a99.h7f0fa5eu.vb8fbi.e8mfzdgrf7g0.groupprograms.in	A	62.75.195.236	192.168.138.158	192.168.138.2
October 25th 2018, 12:01:09.081	ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r9fa f9.e8mfzdgrf7g0.groupprograms.in	A	62.75.195.236	192.168.138.158	192.168.138.2
October 25th 2018, 12:00:58.775	va872g.g90e1h.b8.642b63u.j985a2.x33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in	A	62.75.195.236	192.168.138.158	192.168.138.2
October 25th 2018, 12:00:58.593	comarksecurity.com	A	72.34.49.86	192.168.138.158	192.168.138.2
October 25th 2018, 12:00:58.469	7oqnsnzwwnm6zb7y.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	224.0.0.251
October 25th 2018, 12:00:43.098	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251
October 25th 2018, 12:00:35.836	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251
October 25th 2018, 12:00:35.343	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251
October 25th 2018, 12:00:35.169	runlove.us	A	204.152.254.221	192.168.138.158	192.168.138.2
October 25th 2018, 12:00:35.084	va872g.g90e1h.b8.642b63u.j985a2.x33e.37.pa269cc.e8mfzdgrf7g0.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	224.0.0.251
October 25th 2018, 12:00:27.749	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251
October 25th 2018, 12:00:27.376	_googlecast._tcp.local	PTR	–	192.168.66.1	224.0.0.251