HCP Runbook 1

Investigating Alerts

Date of Publish: 2019-04-09

https://docs.hortonworks.com

Contents

Investigating Alerts

The Alerts user interface frequently produces large amounts of data. You can use features of the Alerts UI to refine and investigate the alert information to identify malicious events.

Filter Alerts

The first Alerts UI feature you can use to focus your data is **Filters**. You can use **Filters** to choose the type of data you are viewing.

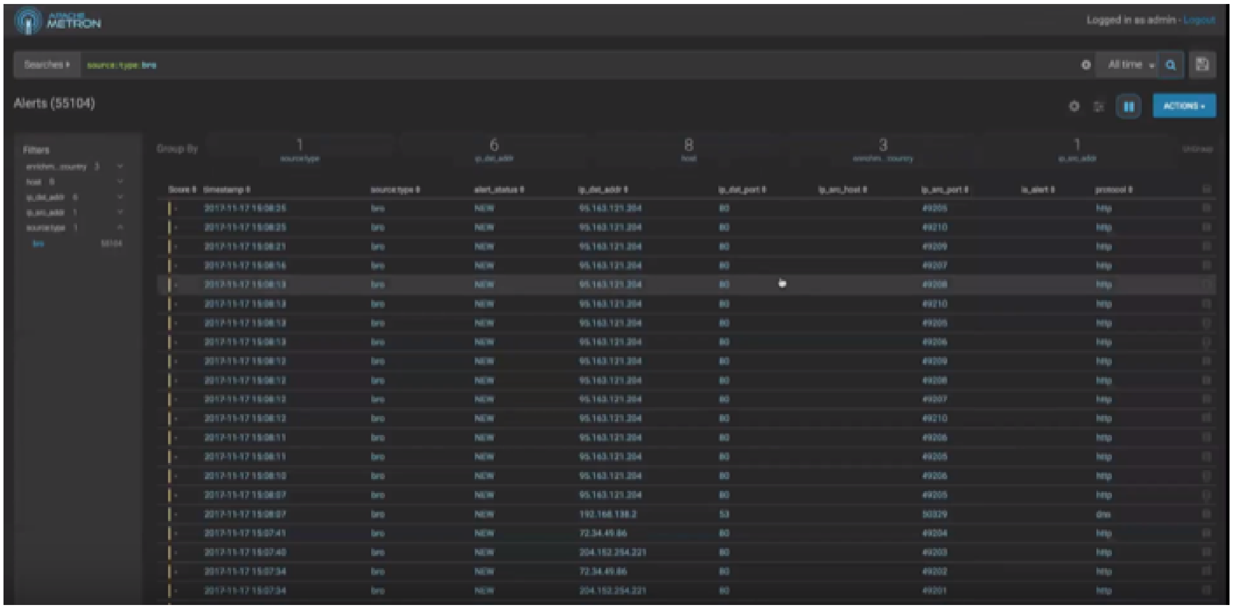
Procedure

1. In the **Filters** panel on the left of the window, click the Bro filter.

   The central panel of the Alerts UI displays all of the Bro data it has received.

   Note:

   Next to the Bro filter, the UI displays the total number of Bro alerts.



source:type:bro

Alerts (55104)

Filters

enrichm...country 3

host 8

ip_dst_addr 6

ip_src_addr 1

source.type 1

bro 55104

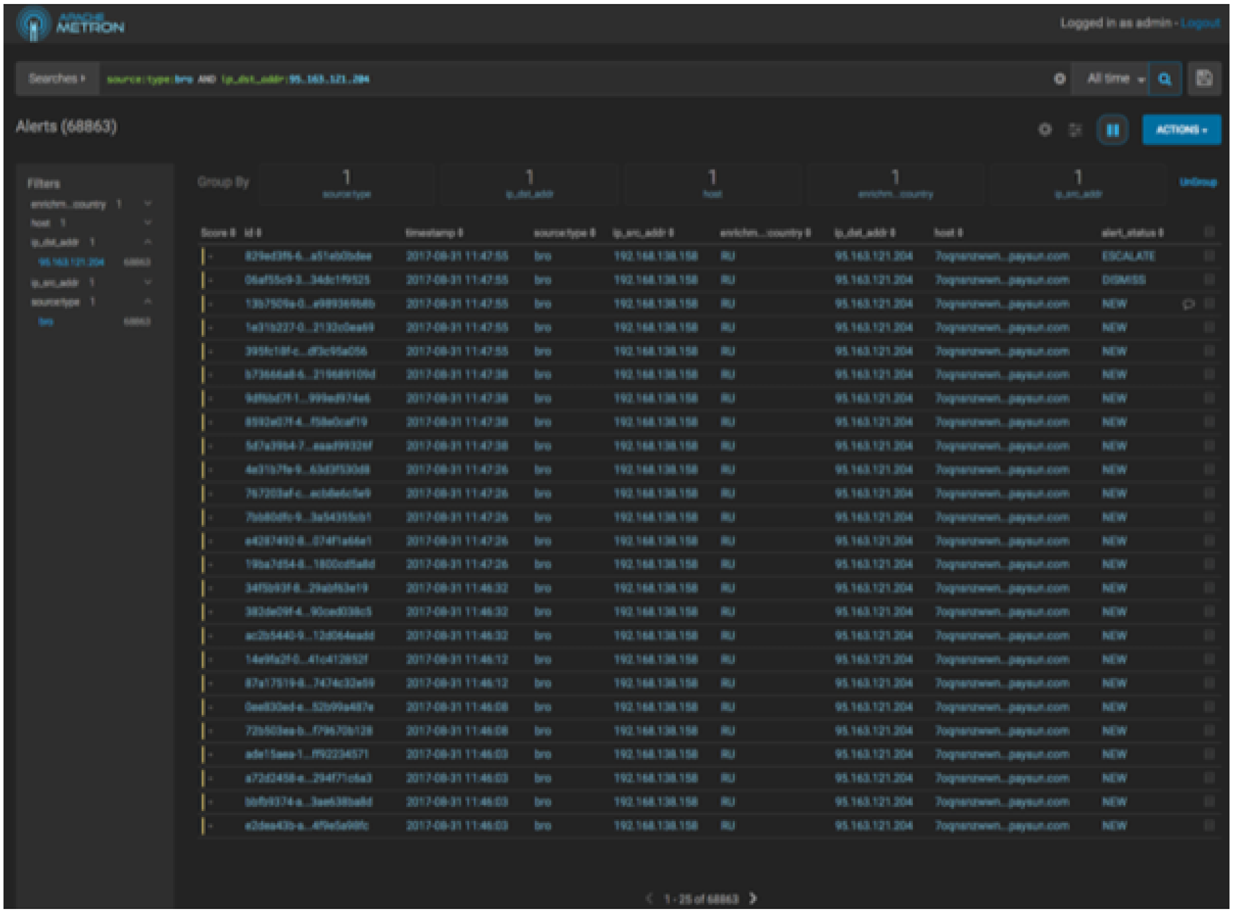
Group By: 1 source.type | 6 ip_dst_addr | 8 host | 3 enrichm...country | 1 ip_src_addr

Score	timestamp	source.type	alert_status	ip_dst_addr	ip_dst_port	ip_src_host	ip_src_port	is_alert	protocol
-	2017-11-17 15:08:25	bro	NEW	95.163.121.204	80		49205		http
-	2017-11-17 15:08:25	bro	NEW	95.163.121.204	80		49210		http
-	2017-11-17 15:08:21	bro	NEW	95.163.121.204	80		49209		http
-	2017-11-17 15:08:16	bro	NEW	95.163.121.204	80		49207		http
-	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80		49208		http
-	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80		49210		http
-	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80		49205		http
-	2017-11-17 15:08:13	bro	NEW	95.163.121.204	80		49206		http
-	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80		49209		http
-	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80		49208		http
-	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80		49207		http
-	2017-11-17 15:08:12	bro	NEW	95.163.121.204	80		49210		http
-	2017-11-17 15:08:11	bro	NEW	95.163.121.204	80		49206		http
-	2017-11-17 15:08:11	bro	NEW	95.163.121.204	80		49205		http
-	2017-11-17 15:08:10	bro	NEW	95.163.121.204	80		49206		http
-	2017-11-17 15:08:07	bro	NEW	95.163.121.204	80		49205		http
-	2017-11-17 15:08:07	bro	NEW	192.168.138.2	53		50329		dns
-	2017-11-17 15:07:41	bro	NEW	72.34.49.86	80		49204		http
-	2017-11-17 15:07:40	bro	NEW	204.152.254.221	80		49203		http
-	2017-11-17 15:07:34	bro	NEW	72.34.49.86	80		49202		http
-	2017-11-17 15:07:34	bro	NEW	204.152.254.221	80		49201		http

2. You can continue to apply filters to the alerts displayed in the **Alerts** window to further refine the alerts list.

   As you select filters and facets, they are displayed in the **Searches** field.

   For example, in the following figure, we've applied the source.type filter with the bro facet and then the ip_dst_addr filter with the IP address 95.163.121.204.



source:type:bro AND ip_dst_addr:95.163.121.204

Alerts (68863)

Filters

enrichm...country	1	
host	1	
ip_dst_addr	1	
95.163.121.204		68863
ip_src_addr	1	
sourcetype	1	
bro		68863

Group By

1	1	1	1	1
sourcetype	ip_dst_addr	host	enrichm...country	ip_src_addr

Score	id	timestamp	source:type	ip_src_addr	enrichm...country	ip_dst_addr	host	alert_status
-	829ed3f6-6...a51eb0bdee	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	ESCALATE
-	06af55c9-3...34dc1f9525	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	DISMISS
-	13b7509a-0...e989369b8b	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	1e31b227-0...2132c0ea69	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	395fc18f-c...df3c95a056	2017-08-31 11:47:55	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	b73666a8-6...219689109d	2017-08-31 11:47:38	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	9df6bd7f-1...999ed974e6	2017-08-31 11:47:38	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	8592e07f-4...f58e0caf19	2017-08-31 11:47:38	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	5d7a39b4-7...eaad99326f	2017-08-31 11:47:38	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	4e31b7fe-9...63d3f530d8	2017-08-31 11:47:26	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	767203af-c...acb8e6c5e9	2017-08-31 11:47:26	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	7bb80dfc-9...3a54355cb1	2017-08-31 11:47:26	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	e4287492-8...074f1a66e1	2017-08-31 11:47:26	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	19ba7d54-8...1800cd5a8d	2017-08-31 11:47:26	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	34f5b93f-8...29abf63e19	2017-08-31 11:46:32	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	382de09f-4...90ced038c5	2017-08-31 11:46:32	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	ac2b5440-9...12d064eadd	2017-08-31 11:46:32	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	14e9fa2f-0...41c412852f	2017-08-31 11:46:12	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	87a17519-8...7474c32e59	2017-08-31 11:46:12	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	0ee830ed-e...52b99a487e	2017-08-31 11:46:08	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	72b503ea-b...f79670b128	2017-08-31 11:46:08	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	ade15aea-1...ff92234571	2017-08-31 11:46:03	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	a72d2458-e...294f71c6a3	2017-08-31 11:46:03	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	bbfb9374-a...3ae638ba8d	2017-08-31 11:46:03	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW
-	e2dea43b-a...4f9e5a98fc	2017-08-31 11:46:03	bro	192.168.138.158	RU	95.163.121.204	7oqnsnzwwn...paysun.com	NEW

‹ 1 - 25 of 68863 ›

3. To clear filters that have been populated to the **Searches** field, click ⊗ (delete icon) at the end of the **Searches** field.

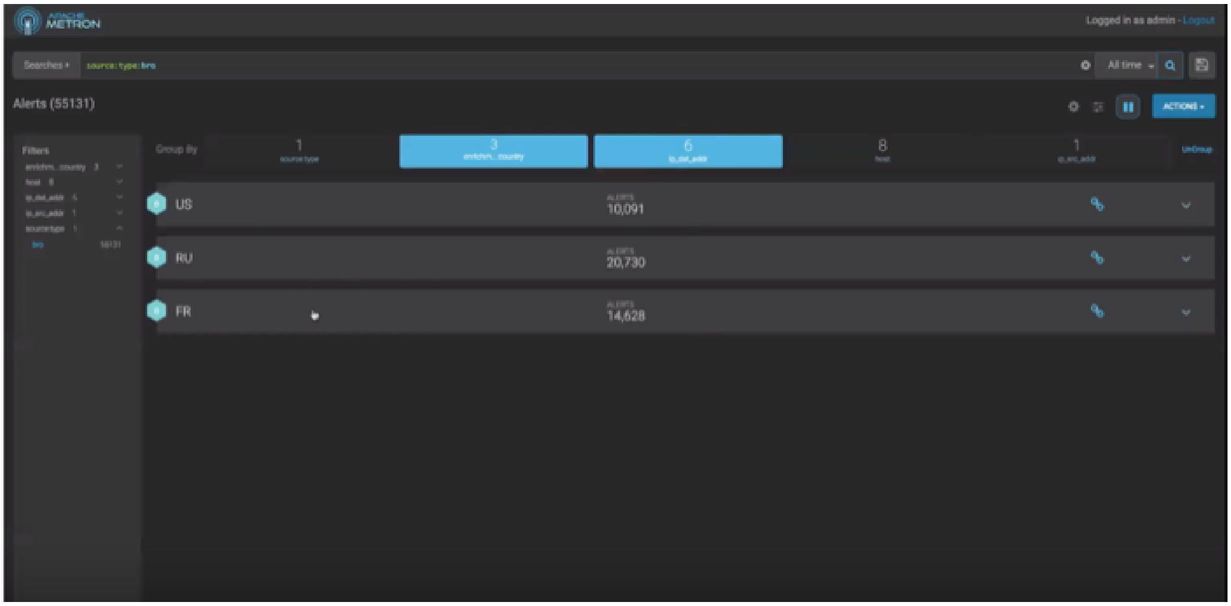
Group Alerts

Frequently, there are a large number of alerts contained in each of the **Filters**. To further refine the alert data, you can use the **Group By** feature. In addition to limiting the type of data you are viewing, you can apply searches, status, etc. to all the alerts in a group at the same time.

Procedure

1. Click **enrichment:country** in the **Group By** section at the top of the UI to group your Bro filtered data by country.

   In the following example, you can see that the alerts are now grouped into three countries: US, RU, and FR.



source:type:bro

Alerts (55131)

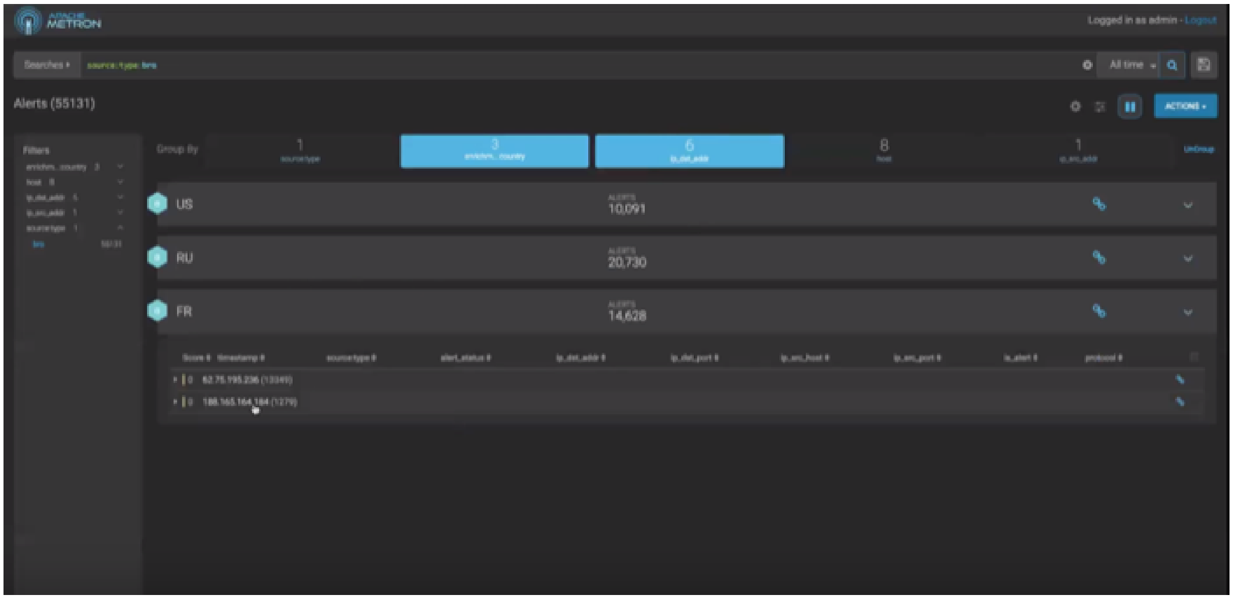
1 source:type	3 enrichm...country	6 ip_dst_addr
8 host	1 ip_src_addr	

US ALERTS 10,091

RU ALERTS 20,730

FR ALERTS 14,628

2. Click on the FR (France) group to see the IP addresses listed for the country:



source:type:bro

Alerts (55131)

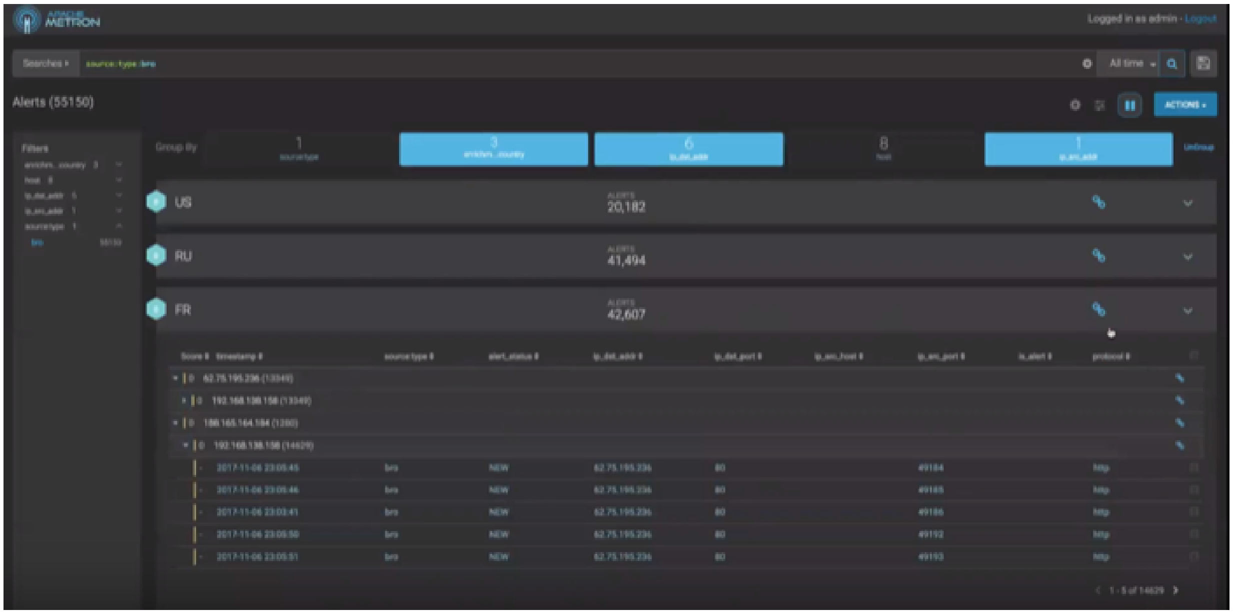
US ALERTS 10,091

RU ALERTS 20,730

FR ALERTS 14,628

Score	timestamp	source:type	alert_status	ip_dst_addr	ip_dst_port	ip_src_host	ip_src_port	is_alert	protocol
0	62.75.195.236 (13349)								
0	188.165.164.184 (1279)								

3. You can click on the IP addresses to display Bro alerts for a specific host:



source:type:bro

Score	timestamp	source:type	alert_status	ip_dst_addr	ip_dst_port	ip_src_host	ip_src_port	is_alert	protocol
0	62.75.195.236 (13349)								
0	192.168.138.158 (13349)								
0	188.165.164.184 (1280)								
0	192.168.138.158 (14629)								
-	2017-11-06 23:05:45	bro	NEW	62.75.195.236	80		49184		http
-	2017-11-06 23:05:46	bro	NEW	62.75.195.236	80		49185		http
-	2017-11-06 23:03:41	bro	NEW	62.75.195.236	80		49186		http
-	2017-11-06 23:05:50	bro	NEW	62.75.195.236	80		49192		http
-	2017-11-06 23:05:51	bro	NEW	62.75.195.236	80		49193		http

4. You can apply search parameters to the grouped information to display more granular information.

Create Meta Groups

Another way you can group filtered alerts is by creating meta alerts. This enables you to deal with the group as a single instance. You can create meta alerts at any of the various levels of groups.

Procedure

1. Select a groups of alerts on which you want to focus, then click

🔗

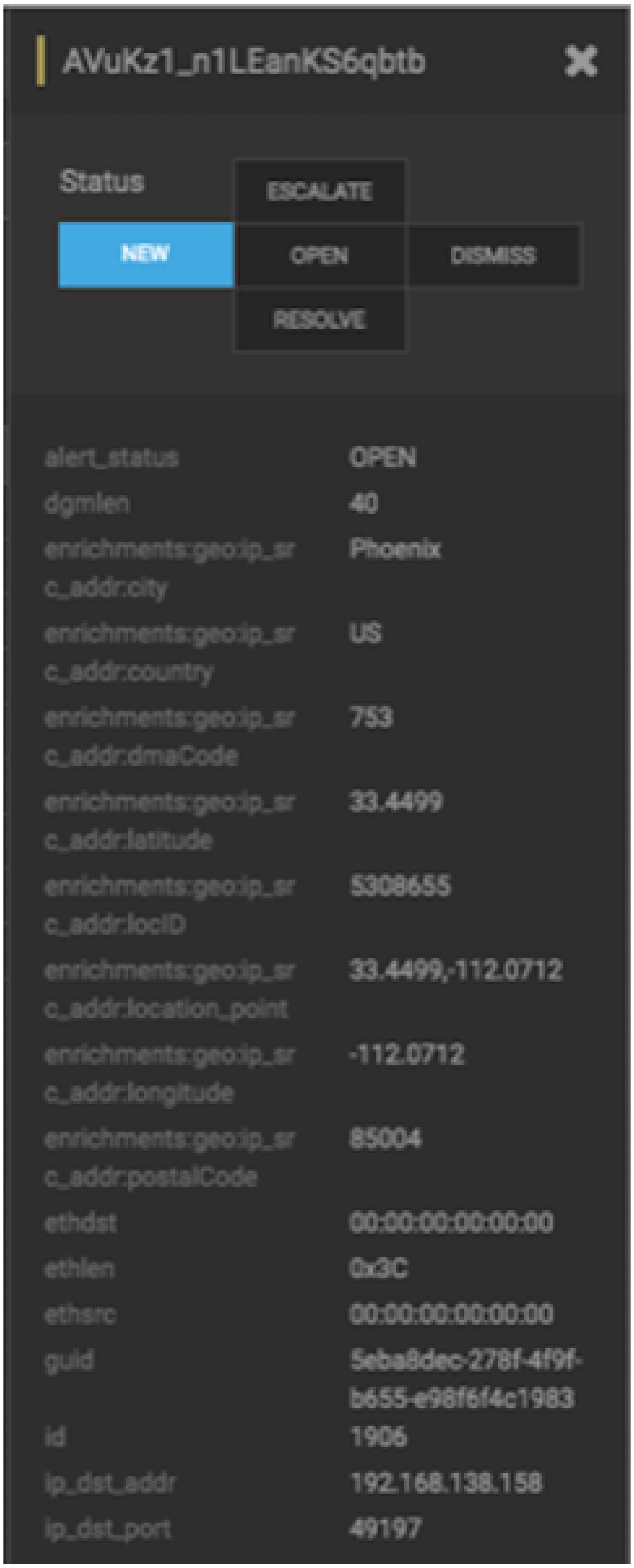
(meta alert icon) and confirm that you wish to create a meta alert.

The meta alert disappears from the tree view. You can still see the meta alert in the alerts table view.

2. You can rename your meta alert by completing the following steps:

a) Display the Alerts UI display panel by clicking on empty space in the meta alert row.

Alerts Information Panel



alert_status	OPEN
dgmlen	40
enrichments:geo:ip_src_addr:city	Phoenix
enrichments:geo:ip_src_addr:country	US
enrichments:geo:ip_src_addr:dmaCode	753
enrichments:geo:ip_src_addr:latitude	33.4499
enrichments:geo:ip_src_addr:locID	5308655
enrichments:geo:ip_src_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_src_addr:longitude	-112.0712
enrichments:geo:ip_src_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f-b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

b) Click the current meta alert name at the top of the panel and enter your new meta alert name.

c) Dismiss the panel by clicking the X in the upper right corner of the panel.

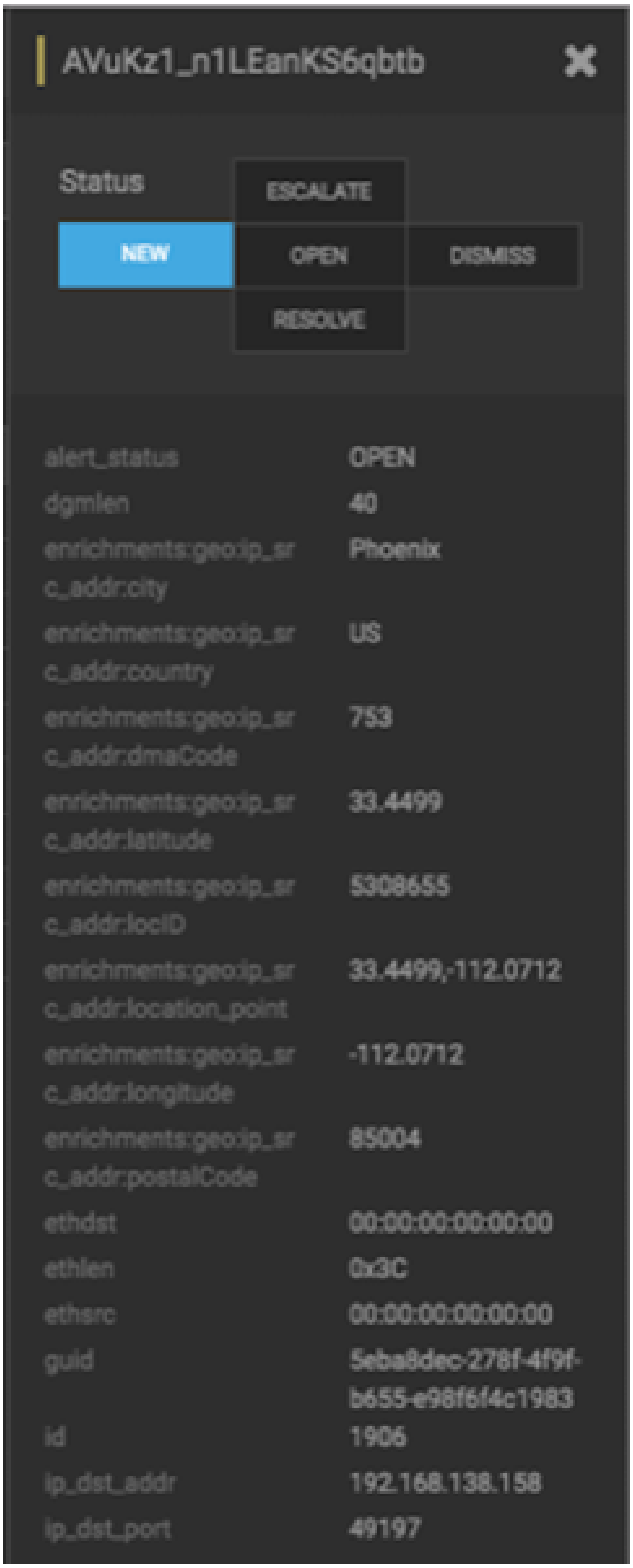
Escalating Alerts

You can escalate one or more alerts at a time to create an event that can be tracked by an external ticketing system.

Procedure

1. Select an alert by clicking on empty space in the alert row.

   The Alerts UI displays a panel listing the status of the alert all available data in Elasticsearch about the alert.



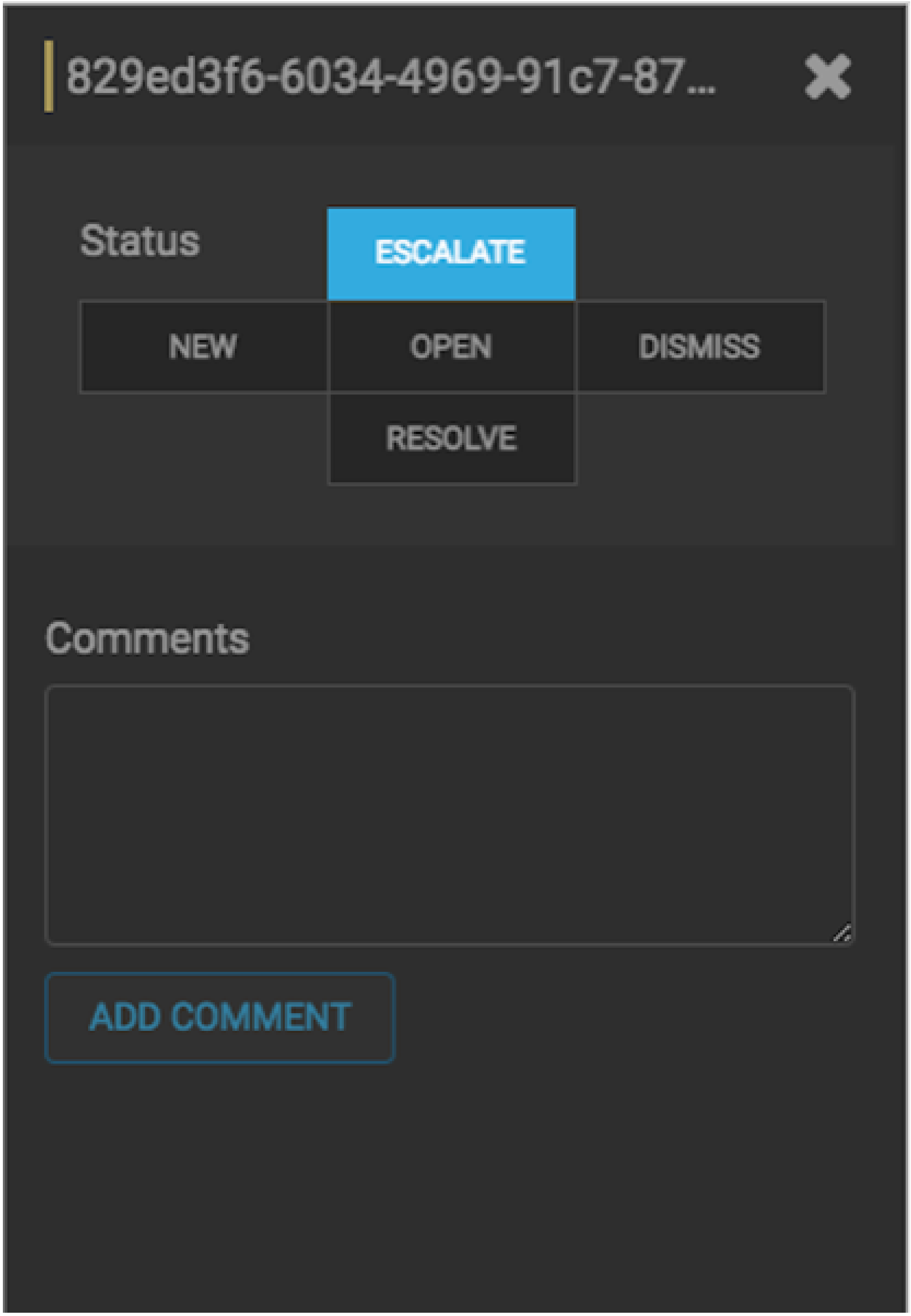
alert_status	OPEN
dgmlen	40
enrichments:geo:ip_src_addr:city	Phoenix
enrichments:geo:ip_src_addr:country	US
enrichments:geo:ip_src_addr:dmaCode	753
enrichments:geo:ip_src_addr:latitude	33.4499
enrichments:geo:ip_src_addr:locID	5308655
enrichments:geo:ip_src_addr:location_point	33.4499,-112.0712
enrichments:geo:ip_src_addr:longitude	-112.0712
enrichments:geo:ip_src_addr:postalCode	85004
ethdst	00:00:00:00:00:00
ethlen	0x3C
ethsrc	00:00:00:00:00:00
guid	5eba8dec-278f-4f9f-b655-e98f6f4c1983
id	1906
ip_dst_addr	192.168.138.158
ip_dst_port	49197

The current alert status is highlighted.

Note:

To manage more than one alert at a time, click the check boxes at the end of alert rows, then select the action you want to perform from the ACTIONS menu.

2. Click **Escalate**.



HCP writes the event to a Kafka escalation topic. An external orchestration software can pick up the event from the topic and use the API to create an incident or append to an existing incident.

3. You can also add a comment to this action by clicking 💬 (Comment button), entering your comment in the **Comments** field, and clicking **ADD COMMENT**.