DASHBOARD AND QUERY CREATION IN SUMOLOGIC SIEM

This document demonstrates the queries used to construct a dashboard in Sumologic SIEM to visualize ingested data.

Jordan Patterson

2024

Dashboard and Query Creation in Sumologic SIEM
Jordan Patterson 2024

Panel-1: Create a table view the top 10 most tried usernames

(_source="klj23-03-authlog" and _collector="klj23-03" failed) | parse "* * *[*]: Failed password for invalid user * from * port * ssh2" as time,h_name,service,pid,username,src_ip,port_no | count by username | top 10 username by _count

This query shows the top 10 most tried usernames. The most tried username is test, followed by admin.

S23C40 JordanPatterson-L6D1P1 -7d

	username	_count
1	test	257
2	admin	251
3	user	235
4	oracle	181
5	git	124
6	ubuntu	101
7	nagios	76
8	tomcat	67
9	ftpuser	65
10	hadoop	65

Panel-2: Filter and find your tried usernames

((_source="klj23-03-authlog" AND _collector="klj23-03"))

| parse "*-*-*-* * *[*]: Failed password for invalid user * from * port * *" as Year,Month,Day,Time,Source,Process,PID,Username,IP,Port,Protocol | count by username | where username matches "jordanpt433"

This query shows the usernames that I tried to login with. I attempted to login 6 times.

S23C40 JordanPatterson-L6D1P2 -30d

	username	_count
1	jordanpt433	6

Dashboard and Query Creation in Sumologic SIEM
Jordan Patterson 2024

Panel-3: Create a map to show failed users' locations

(_source="klj23-03-authlog" and _collector="klj23-03" failed) | parse "* * *[*]: Failed password for invalid user * from * port * ssh2" as time,h_name,service,pid,username,src_ip,port_no | lookup latitude, longitude, country_code, country_name, region, city, postal_code from geo://location on ip = src_ip | count by latitude,longitude

This panel shows the location of failed user login attempts. Most failed attempts seem to come from Europe.

S23C40 JordanPatterson-L6D1P3

Panel-4: Create a list of failed users

(_source="klj23-03-authlog" and _collector="klj23-03" failed) | parse "* * *[*]: Failed password for invalid user * from * port * ssh2" as time,h_name,service,pid,username,src_ip,port_no | count by username | sort by _count

This query shows a list of failed users. The user that failed the most was “admin” which failed 114 times in the last 3 days.

S23C40 JordanPatterson-L6D1P4 -3d

	username	_count
1	admin	114
2	test	113
3	user	92
4	oracle	81
5	git	64
6	ubuntu	58
7	guest	38
8	tomcat	29
9	ftpuser	28
10	nagios	25

1 of 15

Panel-5: Find the valid usernames

(_source="klj23-03-authlog" and _collector="klj23-03") | parse "* * CRON[*]: pam_unix(cron:session): session opened for user *(uid=0) by (uid=0)" as time, hostname, cron, username | count by username

This query shows usernames who were able to open a valid session. The only user I found was root.

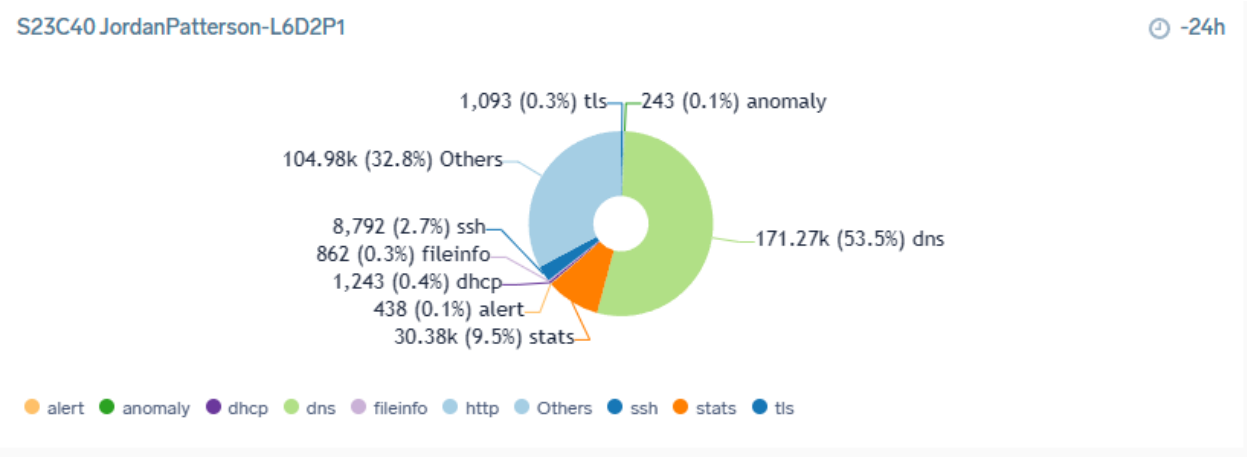
S23C40 JordanPatterson-L6D1P5 -30d

	username	_count
1	root	6,610

Panel-1: Create a Pi chart based on the event type

_sourceCategory="mjolnir/hunt" | count by event_type

With this query we can see that 53.3% of events are related to DNS.



Dashboard and Query Creation in Sumologic SIEM
Jordan Patterson 2024

Panel-2: Create a table for the top 10 destinations under attack (event_type = "alert")

_sourceCategory="mjolnir/hunt" | where event_type="alert" | count by dest_ip | lookup latitude, longitude, country_code, country_name, region, city, postal_code from geo://location on ip=dest_ip | count by country_name | top 10 country_name by _count

This query shows us the top countries under attack. We can see that Canada is #1 with 6 attacks in the last 24hrs.

S23C40 JordanPatterson-L6D2P2

	country_name	_count
1	Canada	6
2	United Kingdom	5
3	United States	4
4		1
5	Thailand	1
6	Sweden	1
7	China	1
8	South Africa	1
9	Hong Kong	1
10	France	1

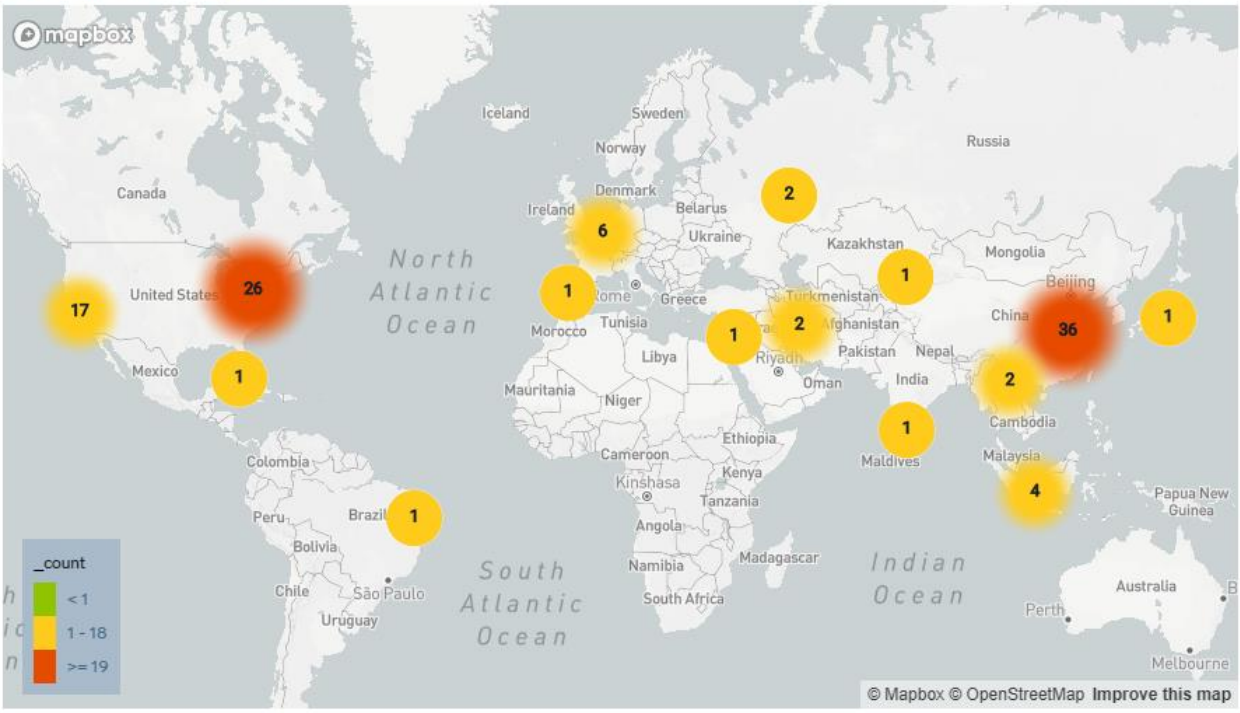
Dashboard and Query Creation in Sumologic SIEM
Jordan Patterson 2024

Panel-3: Visualize on a map source of attack (event_type = "alert")

_sourceCategory="mjolnir/hunt" | where event_type="alert" | count by src_ip | lookup latitude, longitude, country_code, country_name, region, city, postal_code from geo://location on ip=src_ip | count by latitude,longitude

With this query we can see the source of the attack. Most attacks seem to be coming from China and Canada.

S23C40 JordanPatterson-L6D2P3



Panel-4: Show the table of the top 10 attackers

_sourceCategory="mjolnir/hunt" | where event_type="alert" | count by src_ip | top 10 src_ip by _count

This query shows us the top 10 attackers. Since we do not know their names, we have to identify them by IP address.

S23C40 JordanPatterson-L6D2P4

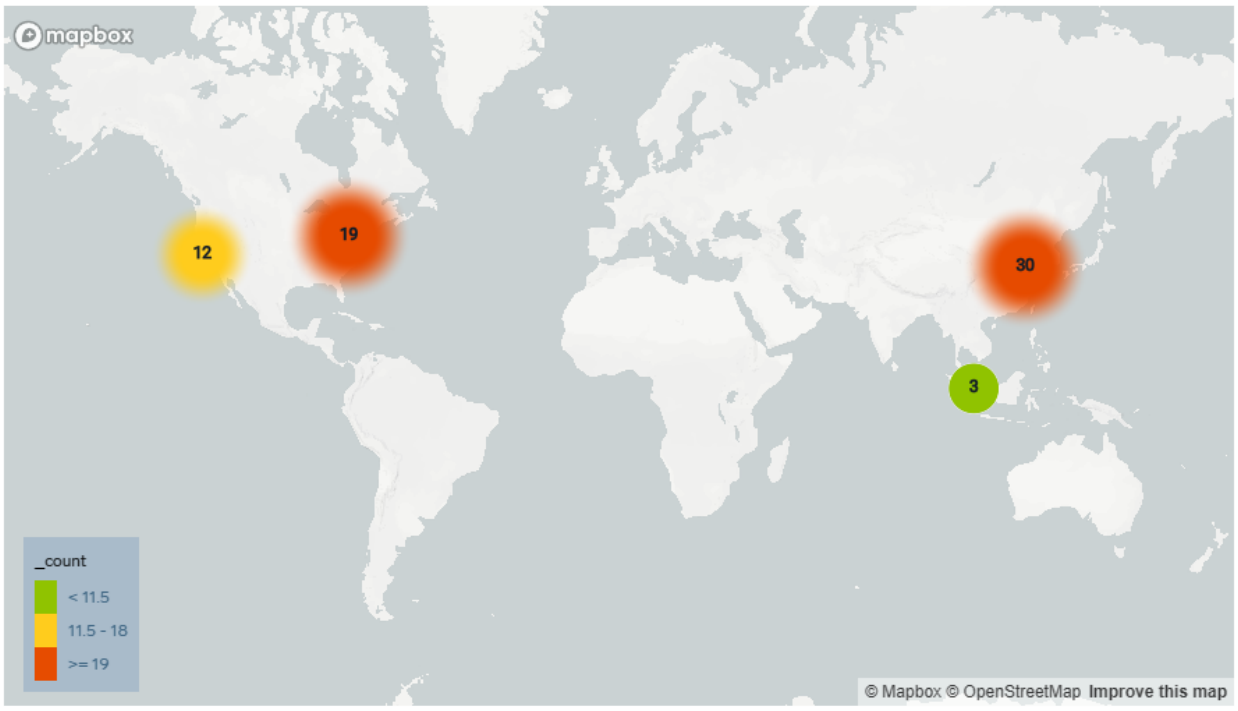
	src_ip	_count
1	2.56.247.174	29
2	185.224.128.184	24
3	117.50.137.84	24
4	192.168.10.144	22
5	114.67.110.206	17
6	5.112.100.55	15
7	2.56.247.173	13
8	218.92.0.107	10
9	64.226.119.125	10
10	218.92.0.118	10

Panel-5: Show the top 10 attackers on the map

_sourceCategory="mjolnir/hunt" | where event_type="alert" | count by src_ip | lookup latitude,longitude,country_code,country_name,region,city,postal_code from geo://location on ip=src_ip | top 10 latitude,longitude

This query will should us the top 10 attackers. The top attackers are coming from China and Canada.

S23C40 JordanPatterson-L6D2P5



Panel-6: Create a table of the top 5 destination ports

_sourceCategory="mjolnir/hunt" | where event_type="alert" | count by dest_port | top 5 dest_port by _count

This query will allow us to know the top services that are being attacked based on which ports are being target the most. We can see that port 22 is being targeted the most which means that the attackers are trying to SSH.

S23C40 JordanPatterson-L6D2P6

	dest_port	_count
1	22	225
2	80	128
3	9987	15
4	443	13
5	19999	9

Panel-7: Create a graph to visualize event trends every 30 minutes (time slice 30m)

_sourceCategory="mjolnir/hunt" | where event_type matches "*" | timeslice 30m | count by _timeslice | sort by _timeslice

This query helps us see at which times most events occur. There is an increase in events at 5am and 9am but then we see the number of events decrease around 19:00.

S23C40 JordanPatterson-L6D2P7