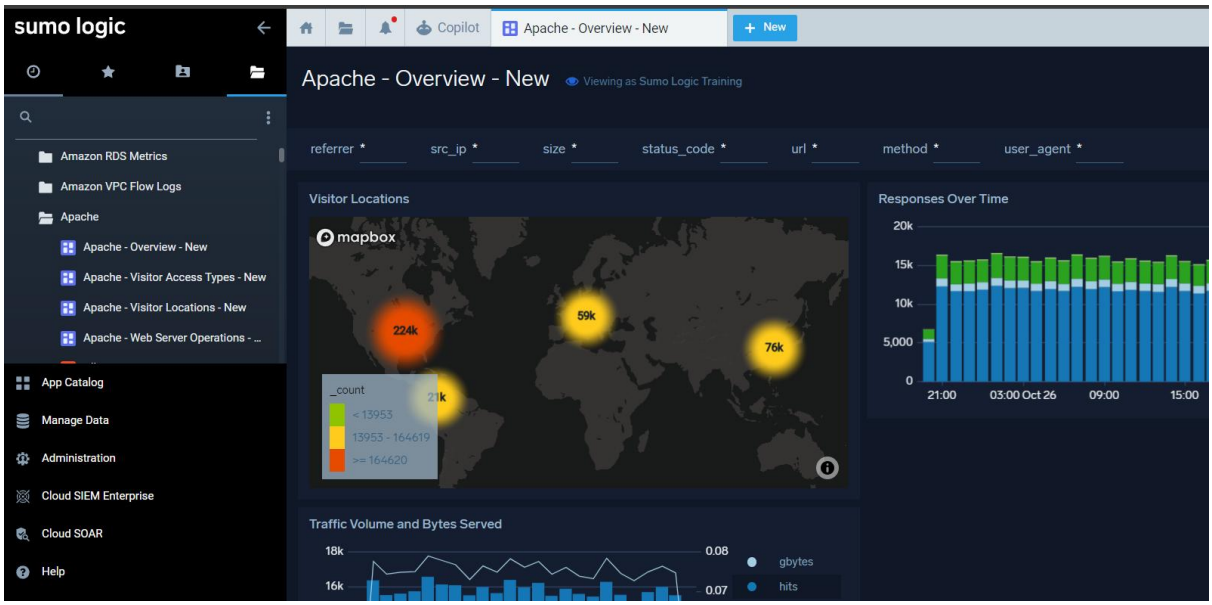
Lab: Monitoring Data by Email (Sumo Logic)

I created an email monitoring alert so the system can automatically send me updates at a scheduled time, even when I am not actively checking the dashboard.

This is important because it allows continuous monitoring without needing to stay logged in or watch the data manually. The alert gives me a full report of the current status, including any unusual activity or changes in trends.

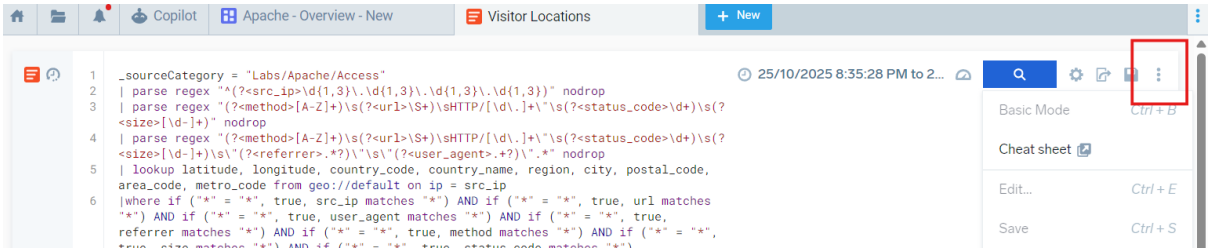
It also helps in early detection of errors, performance issues, or security risks, so I can respond quickly. Email alerts are useful for tracking system health, monitoring traffic behaviour, and staying informed about important events in the environment. Most importantly, they save time and make sure that nothing important is missed during off-hours.

As an example, I selected **Apache** from the library on the left side of the panel. Then I opened **Apps** and chose **Apache**. The main screen displayed several dashboards.

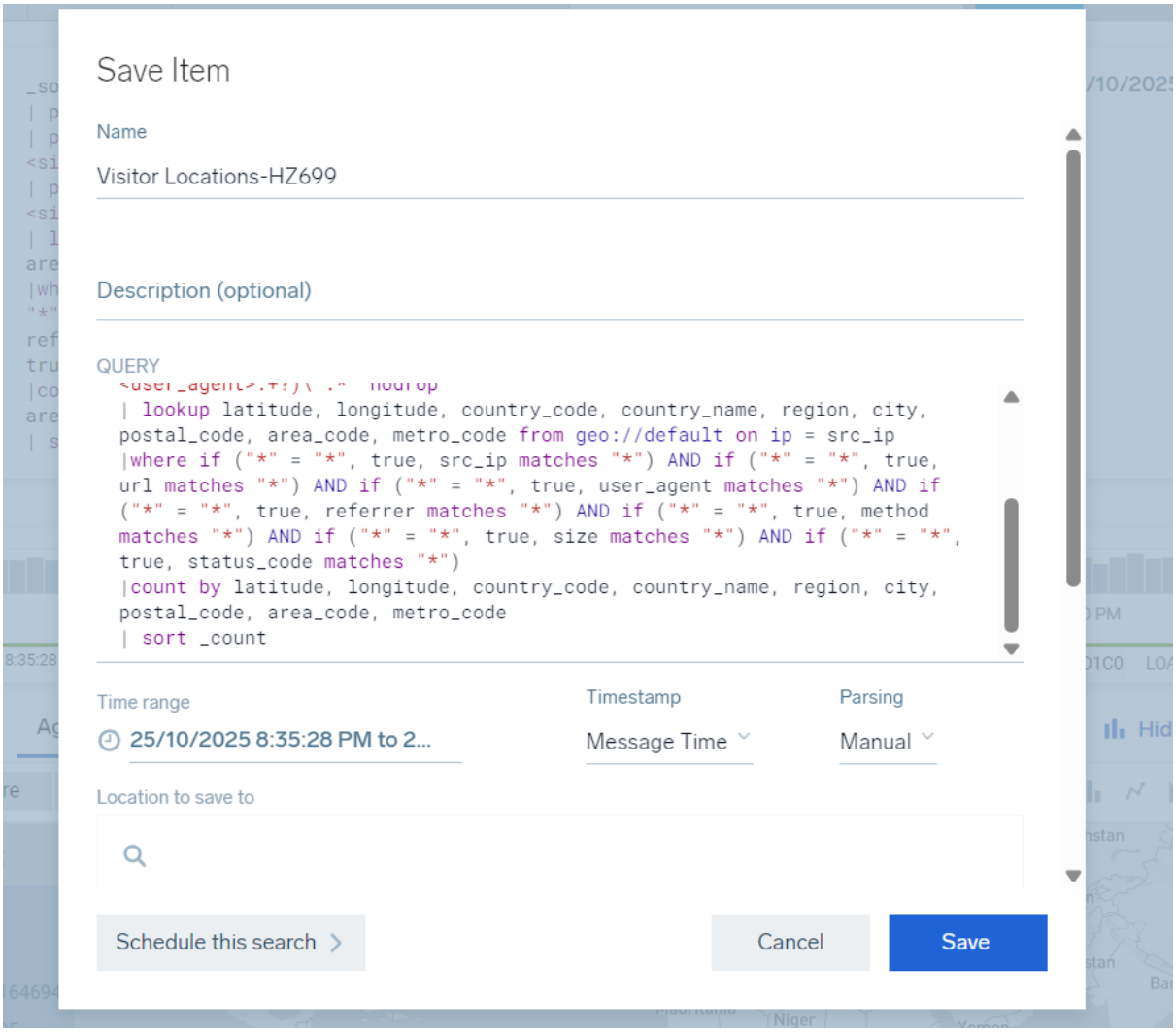


After that, I clicked the three dots on the Visitor Location's panel and selected **Open in Log Search**, which opened the log search in a new window.

On the next window, I clicked the three dots on the right side, and several options appeared.

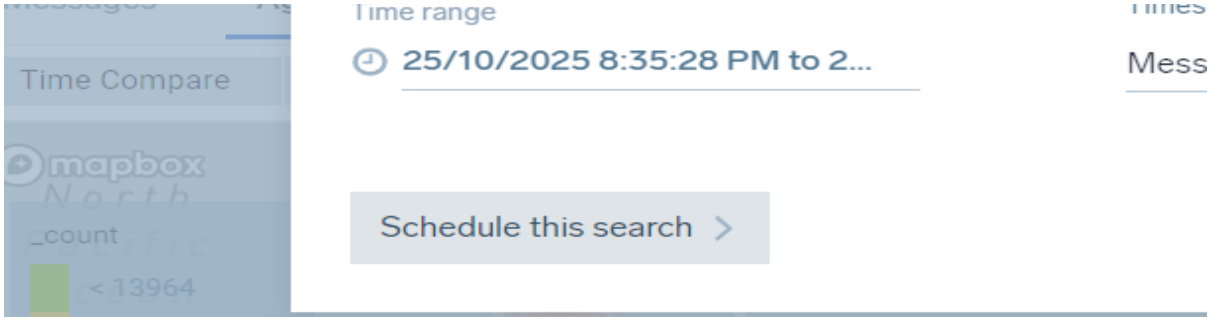


I selected **Save As**, and a small window opened.



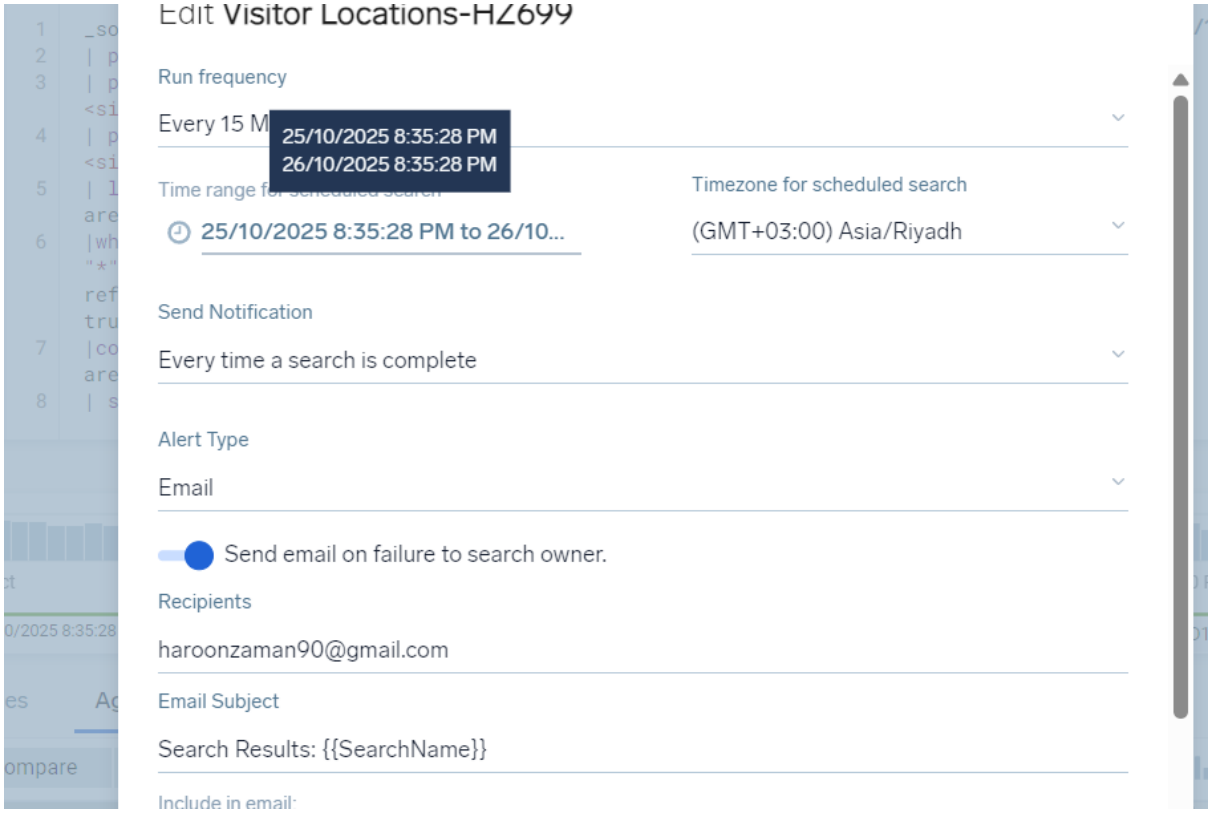
In the small window, you can save the search to your personal library by changing the name and description. The query is also shown, but it does not need any changes at this moment. There are also other important details about the Visitor's Location.

At the bottom left of the window, there is a button called **Schedule this search**, and clicking it moves to the next small window.



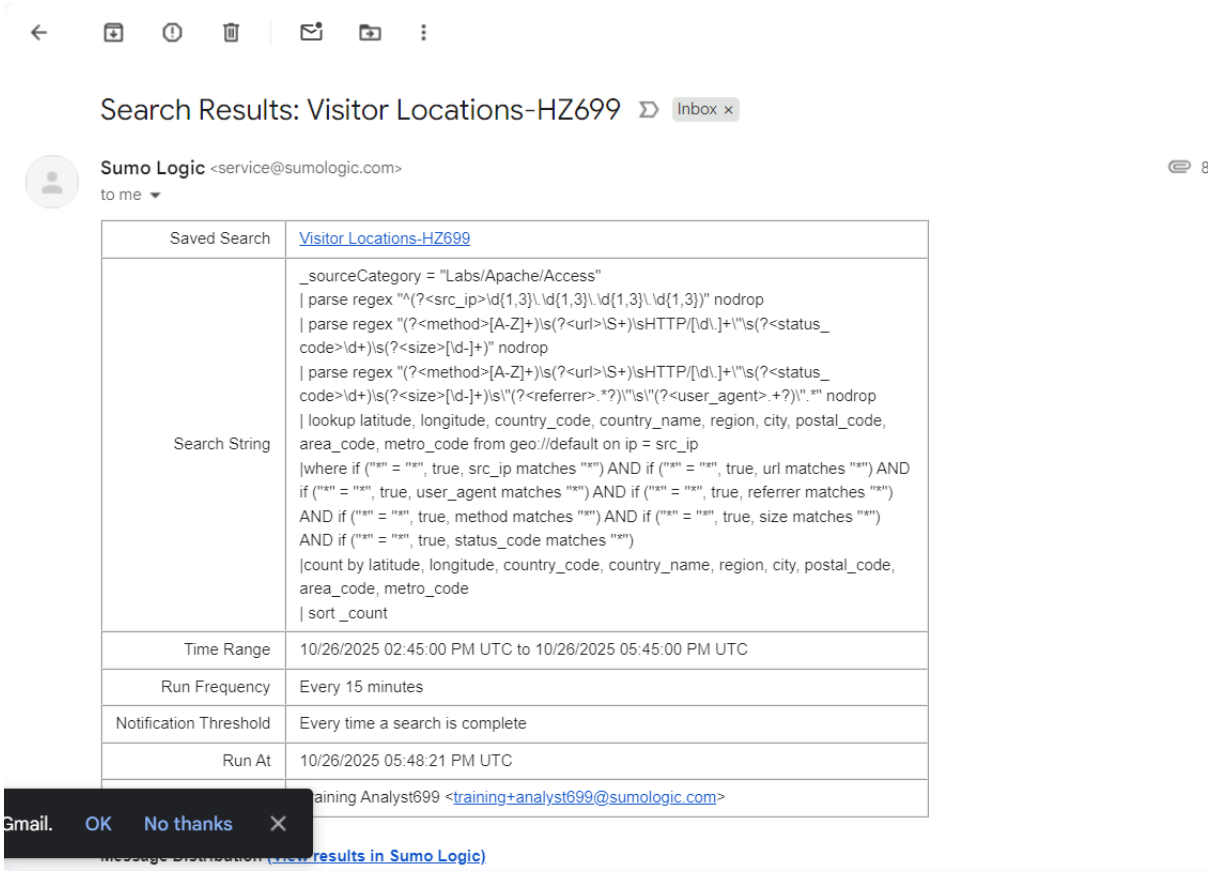
In this window, I selected the **Run Frequency**, which defined how often the monitoring data would be sent to me.

Then I added the email address, and the window displayed all the necessary information that would be sent to my inbox.



After selecting my preferred options in that window, I clicked **Save**, and it was added to my personal library.

As I had selected a run frequency of 15 minutes for my lab, the system started sending me the monitoring emails after the set time passed, as shown in the screenshots.



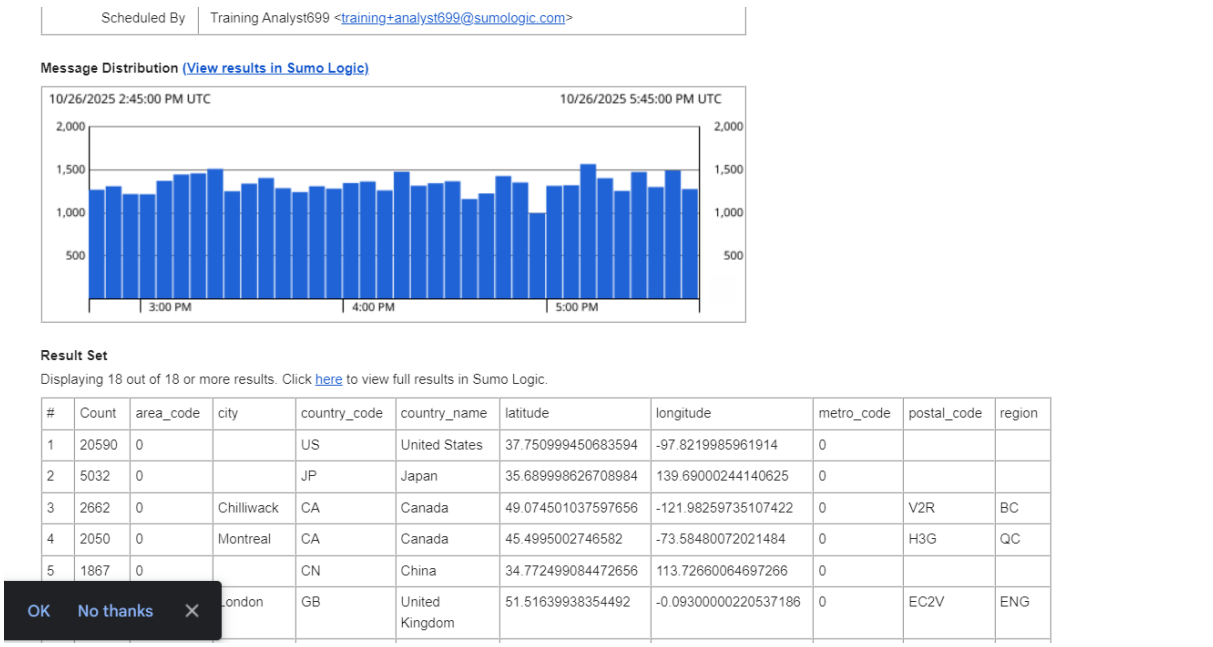
Search Results: Visitor Locations-HZ699 Inbox ×

Sumo Logic <service@sumologic.com>
to me

Saved Search	Visitor Locations-HZ699
Search String	_sourceCategory = "Labs/Apache/Access" | parse regex "^(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" nodrop | parse regex "(?<method>[A-Z]+)\s(?<url>\S+)\sHTTP/[\d\.]+\"\s(?<status_code>\d+)\s(?<size>[\d-]+)" nodrop | parse regex "(?<method>[A-Z]+)\s(?<url>\S+)\sHTTP/[\d\.]+\"\s(?<status_code>\d+)\s(?<size>[\d-]+)\s\"(?<referrer>.*?)\"\s\"(?<user_agent>.+?)\".*" nodrop | lookup latitude, longitude, country_code, country_name, region, city, postal_code, area_code, metro_code from geo://default on ip = src_ip |where if ("*" = "*", true, src_ip matches "*") AND if ("*" = "*", true, url matches "*") AND if ("*" = "*", true, user_agent matches "*") AND if ("*" = "*", true, referrer matches "*") AND if ("*" = "*", true, method matches "*") AND if ("*" = "*", true, size matches "*") AND if ("*" = "*", true, status_code matches "*") |count by latitude, longitude, country_code, country_name, region, city, postal_code, area_code, metro_code | sort _count
Time Range	10/26/2025 02:45:00 PM UTC to 10/26/2025 05:45:00 PM UTC
Run Frequency	Every 15 minutes
Notification Threshold	Every time a search is complete
Run At	10/26/2025 05:48:21 PM UTC
	aining Analyst699 <training+analyst699@sumologic.com>

Gmail. OK No thanks ×

esults in Sumo Logic)



Scheduled By | Training Analyst699 <training+analyst699@sumologic.com>

Message Distribution (View results in Sumo Logic)

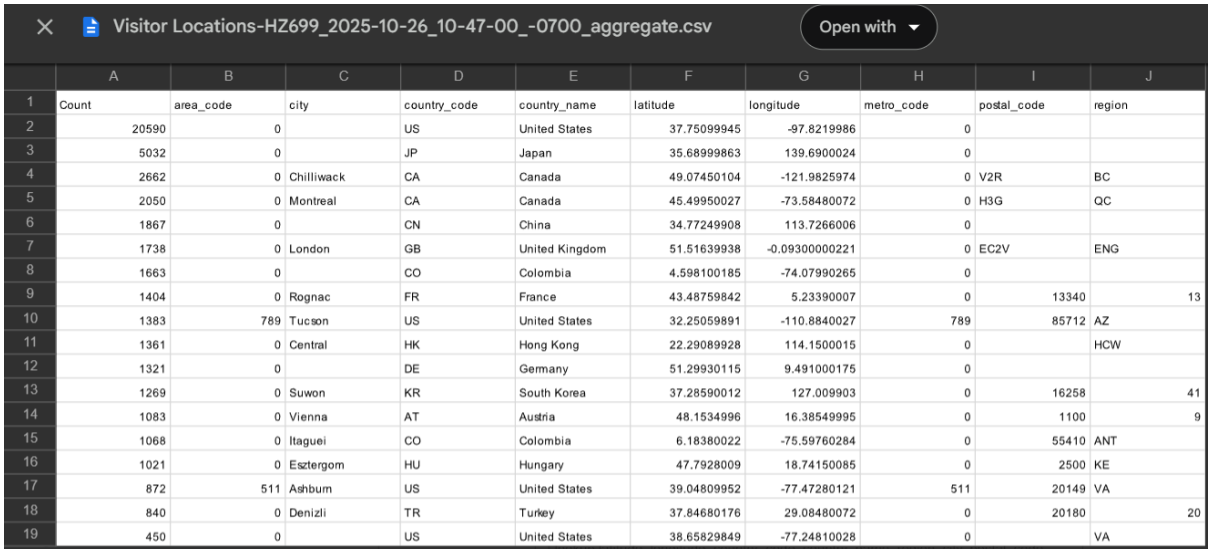
Result Set

Displaying 18 out of 18 or more results. Click here to view full results in Sumo Logic.

#	Count	area_code	city	country_code	country_name	latitude	longitude	metro_code	postal_code	region
1	20590	0		US	United States	37.750999450683594	-97.821985961914	0		
2	5032	0		JP	Japan	35.689998626708984	139.69000244140625	0		
3	2662	0	Chilliwack	CA	Canada	49.074501037597656	-121.98259735107422	0	V2R	BC
4	2050	0	Montreal	CA	Canada	45.499500274658203	-73.58480072021484	0	H3G	QC
5	1867	0		CN	China	34.772499084472656	113.72660064697266	0		
			ondon	GB	United Kingdom	51.51639938354492	-0.09300000220537186	0	EC2V	ENG

OK No thanks ×

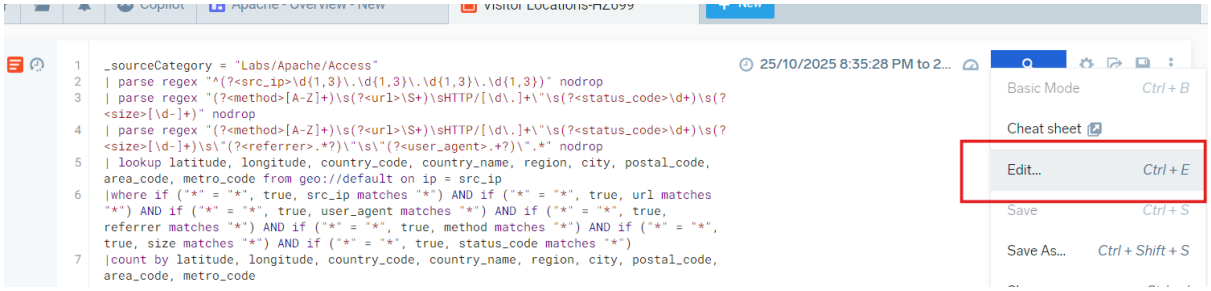
A CSV file with the same data was also attached.



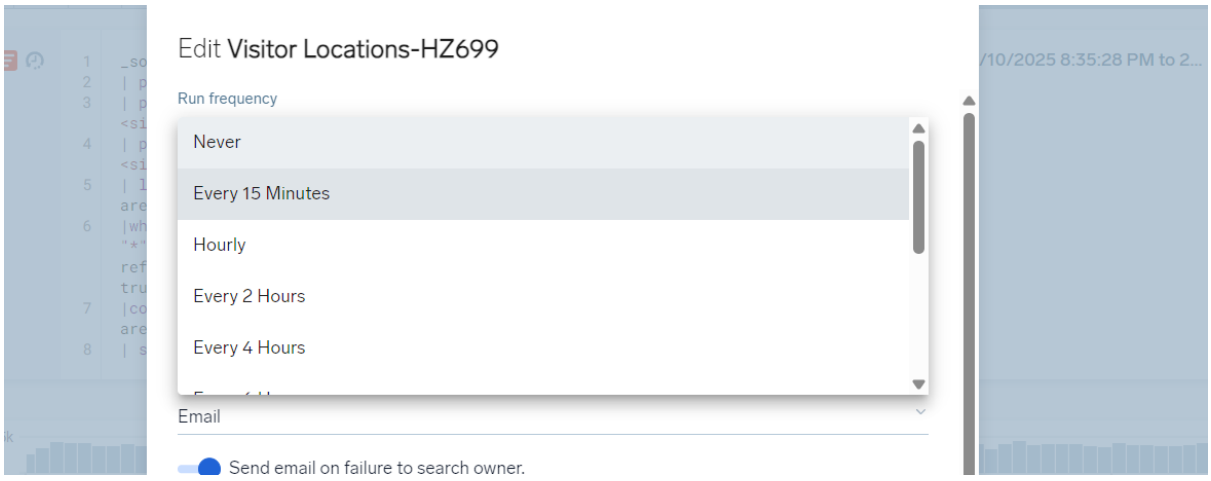
Visitor Locations-HZ699_2025-10-26_10-47-00_-0700_aggregate.csv — Open with

	A	B	C	D	E	F	G	H	I	J
1	Count	area_code	city	country_code	country_name	latitude	longitude	metro_code	postal_code	region
2	20590	0		US	United States	37.75099945	-97.8219986	0		
3	5032	0		JP	Japan	35.68999863	139.6900024	0		
4	2662	0	Chilliwack	CA	Canada	49.07450104	-121.9825974	0	V2R	BC
5	2050	0	Montreal	CA	Canada	45.49950027	-73.58480072	0	H3G	QC
6	1867	0		CN	China	34.77249908	113.7266006	0		
7	1738	0	London	GB	United Kingdom	51.51639938	-0.09300000221	0	EC2V	ENG
8	1663	0		CO	Colombia	4.598100185	-74.07990265	0		
9	1404	0	Rognac	FR	France	43.48759842	5.23390007	0	13340	13
10	1383	789	Tucson	US	United States	32.25059891	-110.8840027	789	85712	AZ
11	1361	0	Central	HK	Hong Kong	22.29089928	114.1500015	0		HCW
12	1321	0		DE	Germany	51.29930115	9.491000175	0		
13	1269	0	Suwon	KR	South Korea	37.28590012	127.009903	0	16258	41
14	1083	0	Vienna	AT	Austria	48.1534996	16.38549995	0	1100	9
15	1068	0	Itaguei	CO	Colombia	6.18380022	-75.59760284	0	55410	ANT
16	1021	0	Esztergom	HU	Hungary	47.7928009	18.74150085	0	2500	KE
17	872	511	Ashburn	US	United States	39.04809952	-77.47280121	511	20149	VA
18	840	0	Denizli	TR	Turkey	37.84680176	29.08480072	0	20180	20
19	450	0		US	United States	38.65829849	-77.24810028	0		VA

After saving, I could also edit the schedule of that search.



I stopped the email alerts by following the same path: **Save As → opens a small window → Run Frequency → Never → clicked Save**, and the alerts were stopped.



Conclusion

In this lab, I learned how to create and manage email monitoring alerts for system data. I understood how to select a dashboard, open a search, save it to my personal library, and schedule it to run automatically. This process is important because it allows continuous monitoring even when I am not actively checking the system. I also learned how to customize the alert frequency, view the data that will be sent, and stop the alerts when needed. Overall,

this lab helped me understand how automated alerts can save time, improve system oversight, and ensure I am always informed about important events and trends in the data.