Data Monitoring

Receiving emails with scheduled reports from a specific log activity in SIEM is beneficial when analysts need regular visibility into trends and low-urgency events that do not require real-time response. Scheduled emails could help with situational awareness and monitoring without overwhelming the security team with constant warnings. There are a couple of scenarios when receiving SIEM scheduled reports is beneficial for the SOC analysts.

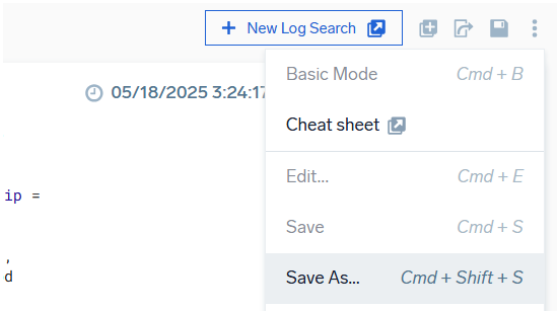
- Threat Trends – Helps analysts identify recurring issues. Alerts could include geo-location of the threat actors or their preferred attack vectors. The security team could then perform some threat intelligence and tune their detection rules.
- User Activity – Helps to monitor user logins and geographic anomalies such as "impossible travel".
- Vulnerability and Patch reports – Helps to control the number of existing vulnerabilities and patch compliance. Patch compliance monitoring also helps to control Service Level Agreement requirements.

Schedule Reports

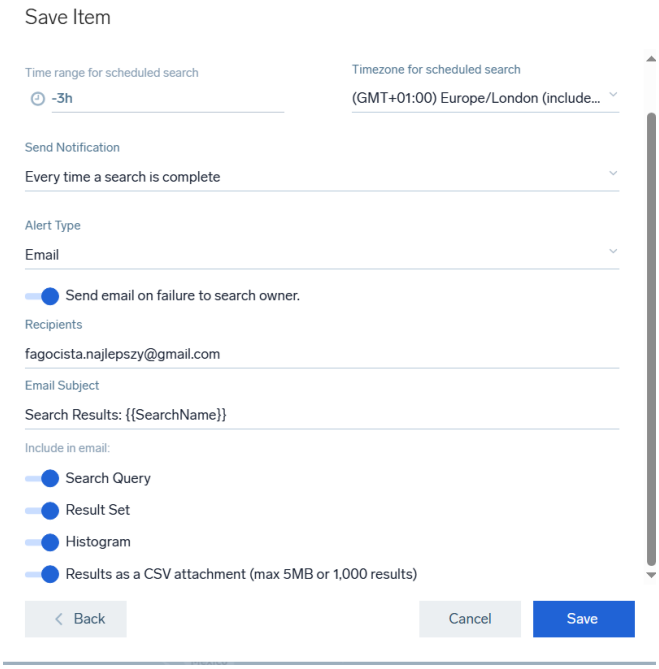
To schedule reports, open the Library, then click on the available folder (in our case, it is the Apache folder) and choose any of the available dashboards.

Choose one of the available options (e.g., visitor locations) and click the three dots in the upper right corner. Then choose the "Open in Log Search" option.

Click the “More actions” Icon and then “Save As…”



On the new pop-up window, change the name of the saved alert, in the lower left corner, click “Schedule this search” and set the frequency to every 15 minutes. Add the email address on which you want to receive the reports and enable “Results as a CSV attachment” option. Click save, and you have just successfully scheduled your email report.



A report received in your email account will look like this, showing the cities with the highest count of visits in the last 3 hours.

Result Set

Displaying 9 out of 9 or more results. Click here to view full results in Sumo Logic.

#	Count	city	country_code	country_name	latitude	longitude	postal_code	region
1	5001	Austin	US	United States	30.28973	-97.76648	78703	South Central
2	4603	New York	US	United States	40.75891	-73.97902	10020	Northeast
3	3966	Secaucus	US	United States	40.77826	-74.06453	07094	Mid Atlantic
4	2151		US	United States	37.88	-96.795		
5	1564	Columbus	US	United States	39.99558	-82.99946	43201	Great Lakes
6	1377	Tucson	US	United States	32.21787	-110.96862	85701	Southwest
7	1337	Center Valley	US	United States	40.54134	-75.40535	18034	Mid Atlantic
8	904	Ashburn	US	United States	39.0437	-77.4742	20147	Mid Atlantic
9	391	Council Bluffs	US	United States	41.26192	-95.86762	51501	Midwest