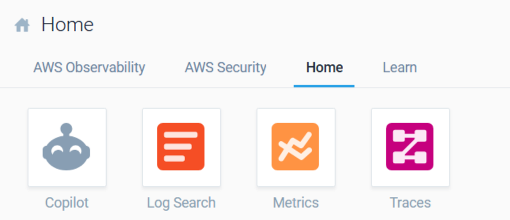
Dashboard Creation

In a walkthrough 1.2, I wrote about the Data Visualization. In this lab, I will cover creating and modifying the dashboards.

Schedule Reports

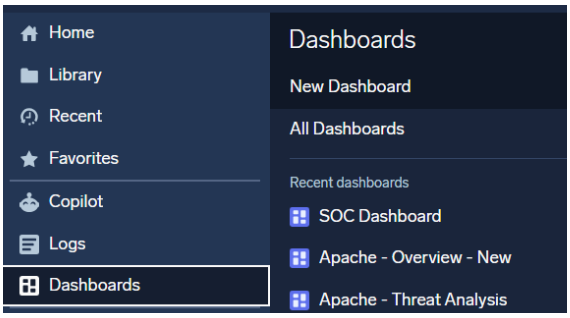
In the main menu, click on the log search logo.



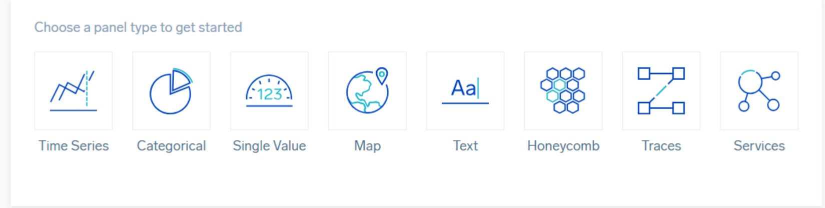
Look for the category of logs. The below query will help with the category choice.

```
_sourcecategory=*
|count by _sourceCategory
| sort by _count desc
```

From the available categories, we can choose “Labs/AWS/CloudTrail”.
In the menu in the left pane, click the “Dashboards” section, and then “New Dashboard”.

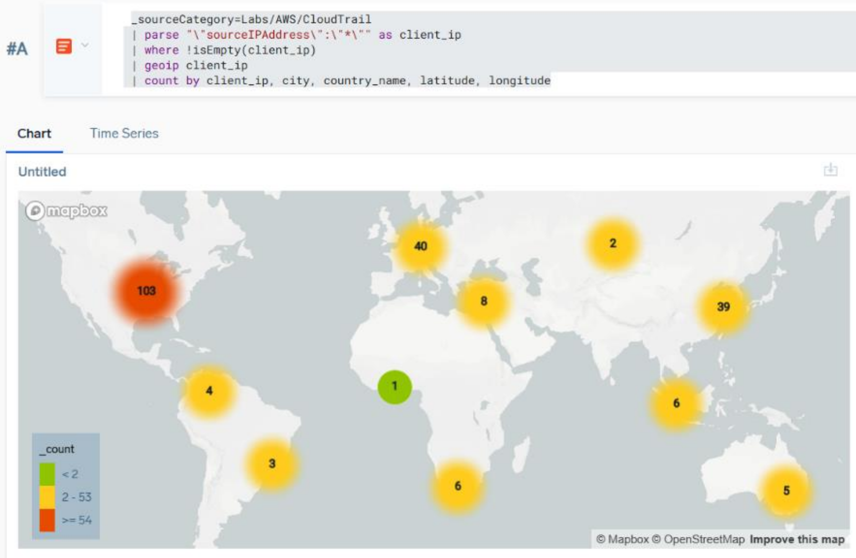


You can choose the layout of a new dashboard. For our first dashboard we want to see the source IP addresses on the map. Choose the map option.



To create our first dashboard, input the following query to see all the IP addresses connecting to CloudTrail.

```
_sourceCategory=Labs/AWS/CloudTrail
| parse "\"sourceIPAddress\":\"*\"" as client_ip
| where !isEmpty(client_ip)
| geoip client_ip
| count by client_ip, city, country_name, latitude, longitude
```



```
_sourceCategory=Labs/AWS/CloudTrail
| parse "\"sourceIPAddress\":\"*\"" as client_ip
| where !isEmpty(client_ip)
| geoip client_ip
| count by client_ip, city, country_name, latitude, longitude
```

Creating a dashboard with a map of source IP addresses can be helpful for visual threat detection. You can quickly spot unusual places for API calls (countries your team does not operate in). For example, you can see Identity and Access Management role change requests come from one of the Middle East countries, while your entire team is based in France. It could also help to detect impossible travel, e.g., the same user accessing AWS from Paris, and 5 minutes later from Hong Kong. That could potentially reveal stolen API keys. Visualization helps SOC analysts to triage threats more effectively and prioritize investigations.

The next dashboard will be a table based on the TOP 10 failed logins. From the Panel Settings option, choose categorical, and below, in the chart type, choose Table. Execute the query below.

```
_sourceCategory=Labs/AWS/CloudTrail
   | json field=_raw "userIdentity.userName" as actor
   | json field=_raw "eventType" as event_type
   | json field=_raw "responseElements.ConsoleLogin" as
   result
   | json field=_raw "eventName" as event_name
   | where actor matches "*"
   | where !isEmpty(actor)
   | where !isEmpty(event_type)
   | where result = "Failure"
   | where event_type = "AwsConsoleSignIn"
   | timeslice 3h
   | count by _timeslice,actor,event_type,event_name,result
   | top 10 actor by _count,_timeslice,event_type,result
```

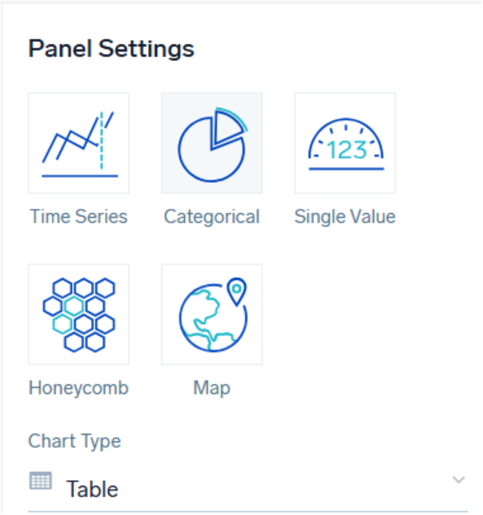
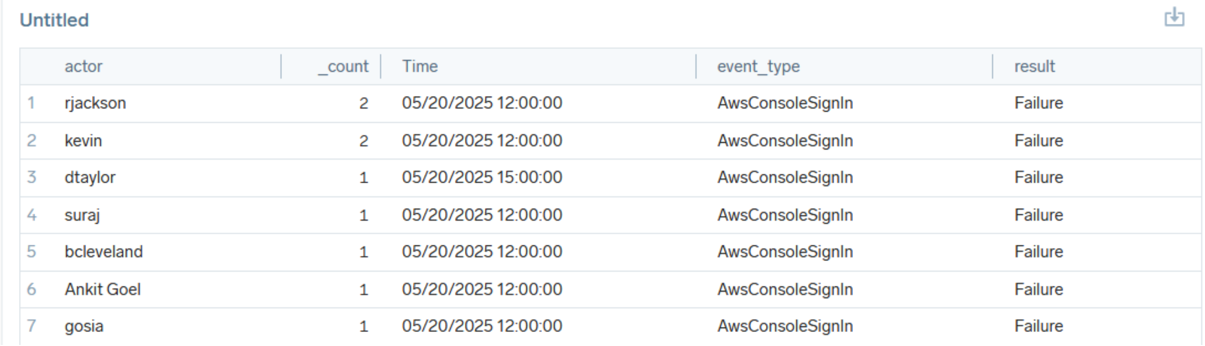


Chart Type

Table

As a result, we will see a table with failed login attempts within the last 3 hours.


Untitled

	actor	_count	Time	event_type	result
1	rjackson	2	05/20/2025 12:00:00	AwsConsoleSignIn	Failure
2	kevin	2	05/20/2025 12:00:00	AwsConsoleSignIn	Failure
3	dtaylor	1	05/20/2025 15:00:00	AwsConsoleSignIn	Failure
4	suraj	1	05/20/2025 12:00:00	AwsConsoleSignIn	Failure
5	bcleveland	1	05/20/2025 12:00:00	AwsConsoleSignIn	Failure
6	Ankit Goel	1	05/20/2025 12:00:00	AwsConsoleSignIn	Failure
7	gosia	1	05/20/2025 12:00:00	AwsConsoleSignIn	Failure

A table showing failed login attempts can point a SOC analyst to suspicious access attempts. When you notice an unusually high count of failed login attempts, that shows that your organization could have been a target of a brute-force attack. The “count” column can help you identify which account is being used the most for this type of attack, allowing you to contact the account owner and suggest a password change. The “Actor” column also helps to identify login attempts using deactivated accounts. That could be an ex-employee trying to gain access to the system with the intention of stealing data.

Data visualization helps the SOC Analysts follow real-time events, enabling them to react fast to potential data breaches. The correct configuration of dashboards can be critical in maintaining strong security within the organization’s IT environment.