_sourceCategory in Sumo Logic is a metadata tag that helps to organize, search, and manage logs effectively. It is a user-defined tag assigned to a log source when configuring it.

Why is it important?

- It helps you structure and manage logs (e.g., Symantec/Firewall or AWS/CloudTrail)
- It helps to schedule alerts and create dashboards utilising only relevant data

Examples

- System Logs (prod/os/linux/syslog)
- Application Logs (prod/app/nodejs)
- Cloud Logs (prod/aws/cloudtrail)

In Sumo Logic, operators like AND, OR, * are responsible for filtering search queries. Here are examples of how to use each effectively.

AND Operator

- Refines the search, requiring both conditions to be true.
- Common use could be '_sourceCategory=prod/web/apache AND 404', requiring logs to be both from the Apache web server and containing the number 404.

OR Operator

- It helps to widen the search results, requiring just one of the conditions to be true.
- Common use could be '_sourceCategory=prod/web/apache AND (404 OR 500)', requiring logs to be from the Apache web server containing either number 404 or 500.

* Operator

- It is used to match multiple characters (wildcard)
- Common use could be '_sourceCategory=prod/web/*' returning logs from any source category starting with 'prod/web/'.

LiveTail is a real-time log streaming feature that allows SOC analysts to see the log messages as they are ingested. It allows you to watch logs from multiple sources simultaneously.