



# Sumo Logic Librarian

## Customer Value Presentation

[wschmidt@sumologic.com](mailto:wschmidt@sumologic.com)

November 3, 2020

# Sumo Logic Librarian

The screenshot shows the Sumo Logic Librarian interface. At the top, there's a header bar with the Sumo Logic logo, a search bar, and navigation icons. Below the header, a banner reads "Welcome to Sumo Logic Librarian! All changes saved". The main area contains two panels: one on the left with a dark background containing text about data sources and a list of indices, and one on the right with a dark background containing a list of sections. A sidebar on the far left is titled "Untitled".

"Libraries are maps into new territories, grand places of learning and wonder"

Query Librarian uses the power of Sumo Logic to look at Sumo Logic and shows you who uses what data how and when answering questions. To deliver this, we use these Sumo Logic data sources listed below:

- [.index=sumologic\\_volume](#)
- [.index=sumologic\\_audit](#)
- [.index=sumologic\\_audit\\_events](#)
- [.index=sumologic\\_search\\_usage\\_per\\_query](#)

The resulting exploration library has the following sections:

- . Section-100 - [Partitions](#)
- . Section-200 - [Source Categories](#)
- . Section-300 - [Extraction Rules](#)
- . Section-400 - [Saved Views](#)
- . Section-500 - [Lookup Files](#)
- . Section-600 - [Indices](#)
- . Section-700 - [Queries](#)
- . Section-800 - [Documentation](#)
- . Section-900 - [Activity](#)

## Challenges:

- Where to start to read more?
- How to tie activity to efficiency?
- How to find my dependencies?

## Solution:

- Use Sumo to discover Sumo
- Use Sumo to explore your environment
- Single portal to learn more and practice

## Benefits:

- Easy & fast setup
- See Results, Performance and Behavior

# Sumo Logic Librarian

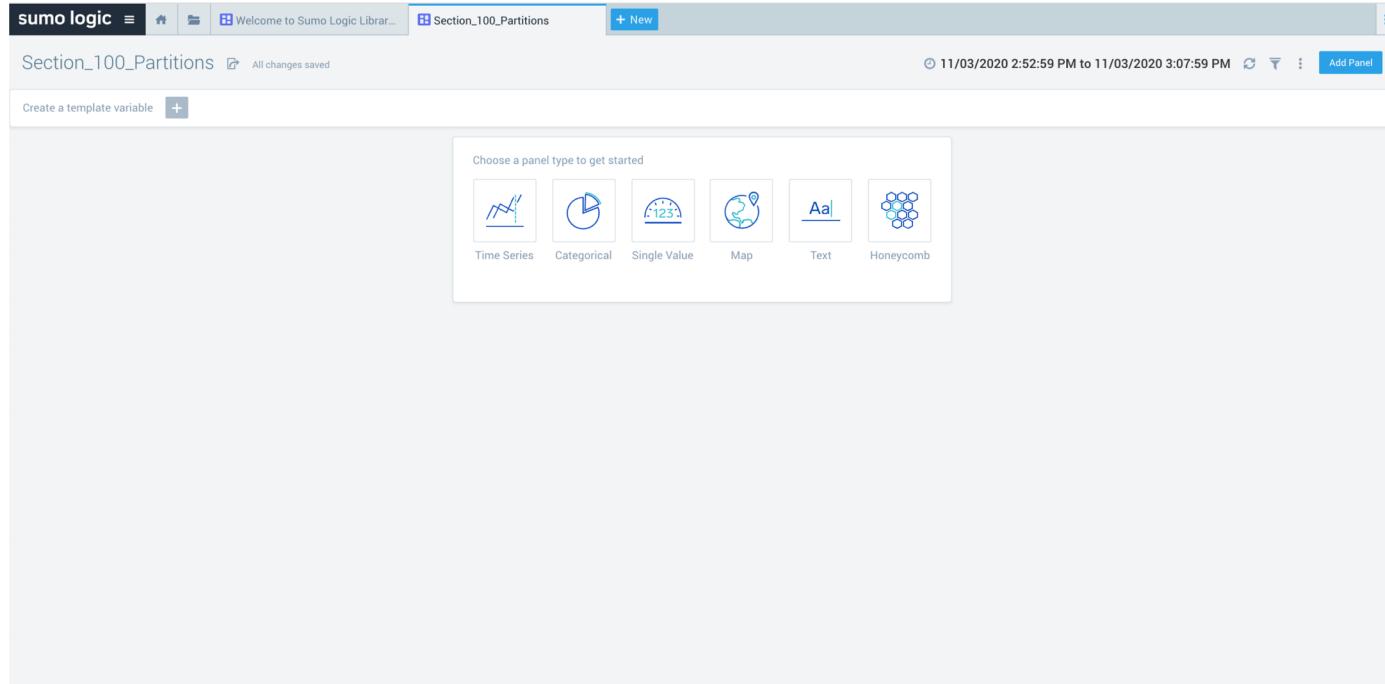
The screenshot shows the Sumo Logic Librarian interface. On the left is a sidebar with a dark background containing various sections like Data Volume, Graham, Sumo Logic Librarian, and App Catalog. The main area has a light gray header with tabs for 'Welcome to Sumo Logic Librarian...', 'Section\_000\_Sumo\_Indices', and '+ New'. Below the header is a message: 'This page shows the list of indices we use in the Query Librarian. The list them here so you can both see the data, and also use sample queries. The list will grow, and evolve as this application evolves.' There are four tables displayed:

- \_index=sumologic\_volume**: Shows data volume feed indices with counts ranging from 1,510 to 2,473.
- \_index=sumologic\_audit**: Shows audit indices with counts ranging from 1 to 89,383.
- \_index=sumologic\_search\_usage\_per\_query**: Shows search usage per query with counts ranging from 113 to 12,949.
- \_index=sumologic\_audit\_events**: Shows audit events with a single entry for MetricsAlertMonitorStatusChanged with a count of 6.

## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

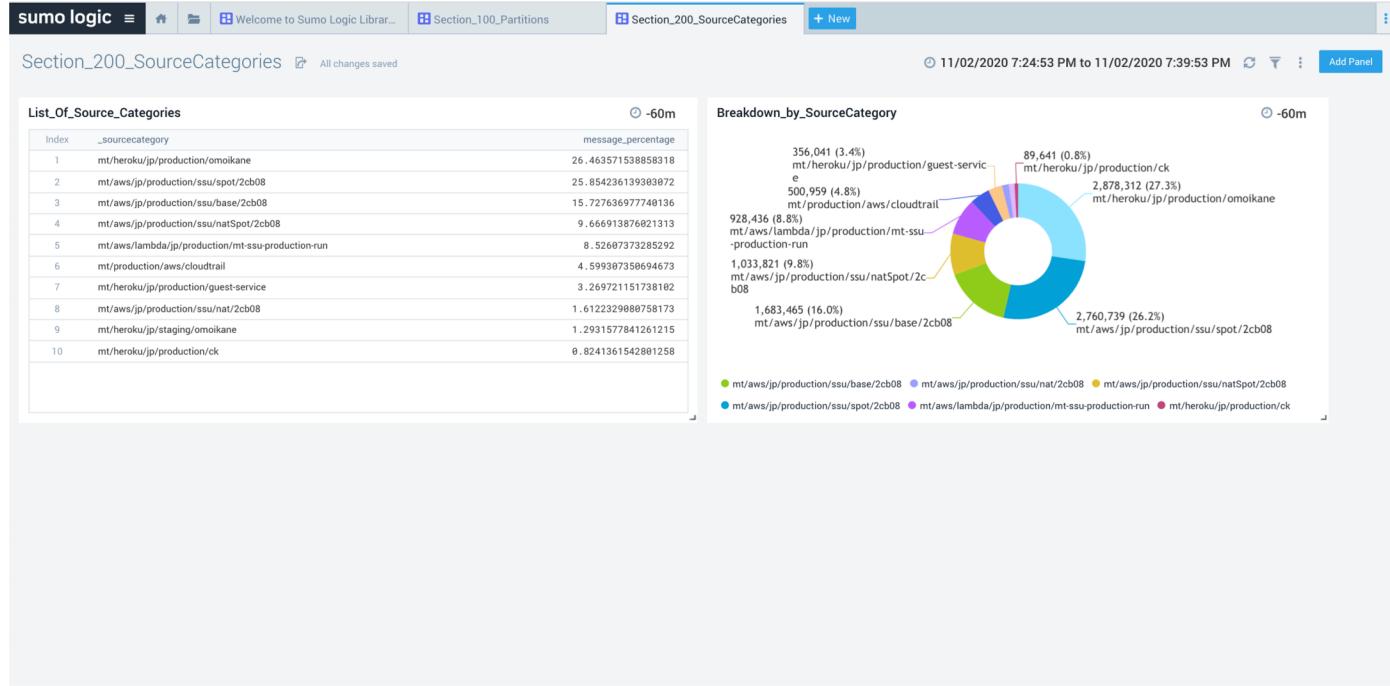
# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

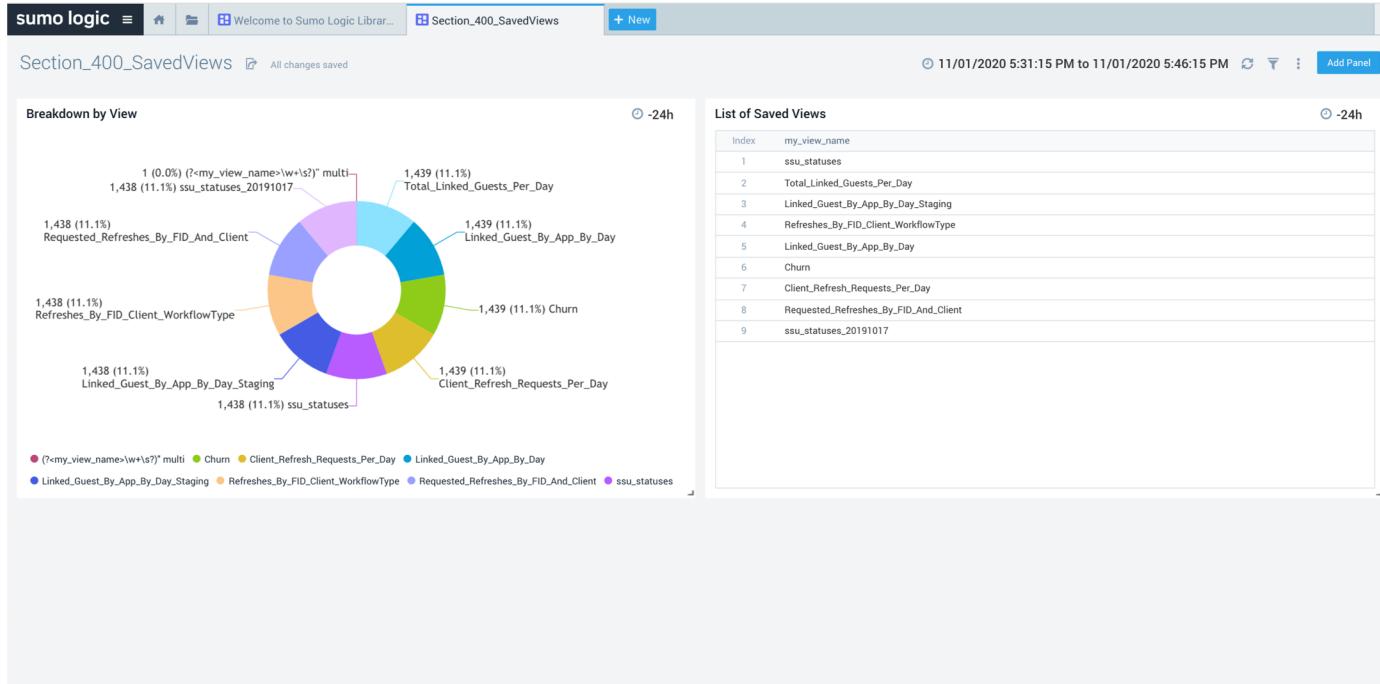
# Sumo Logic Librarian

The screenshot shows a Sumo Logic interface with a top navigation bar featuring icons for search, file, and help, along with the text "Welcome to Sumo Logic Librar...". Below the bar, a tab labeled "Section\_300\_ExtractionRules" is selected. A "New" button is visible in the top right corner. The main content area displays a message: "Currently, we use the Sumo Logic API to get the Extraction Rules. As we progress , we will use a query from the UI to get our list To coordinate the collection of this and other items, we will need to do the following:" followed by a bulleted list: ". Create an API key within Sumo Logic . Install a Collector so we can run a scripted source . install and configure a script source to get the collector information".

## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

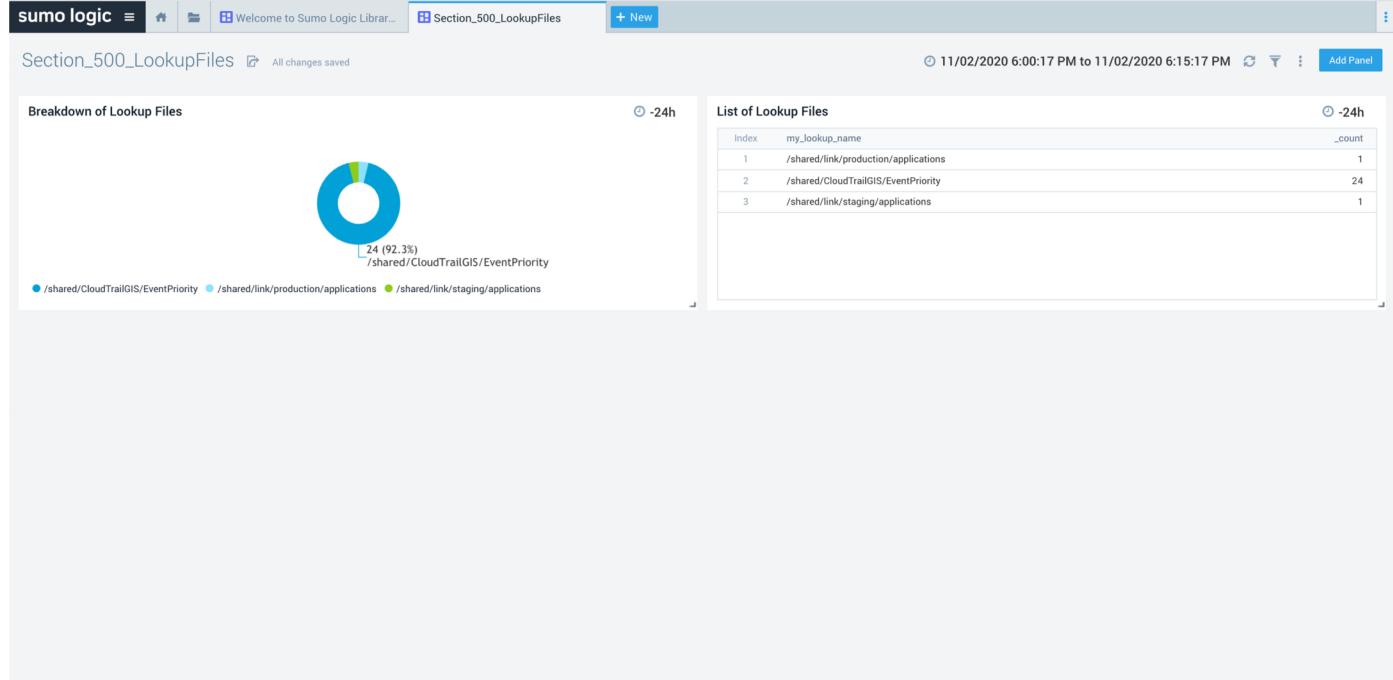
# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

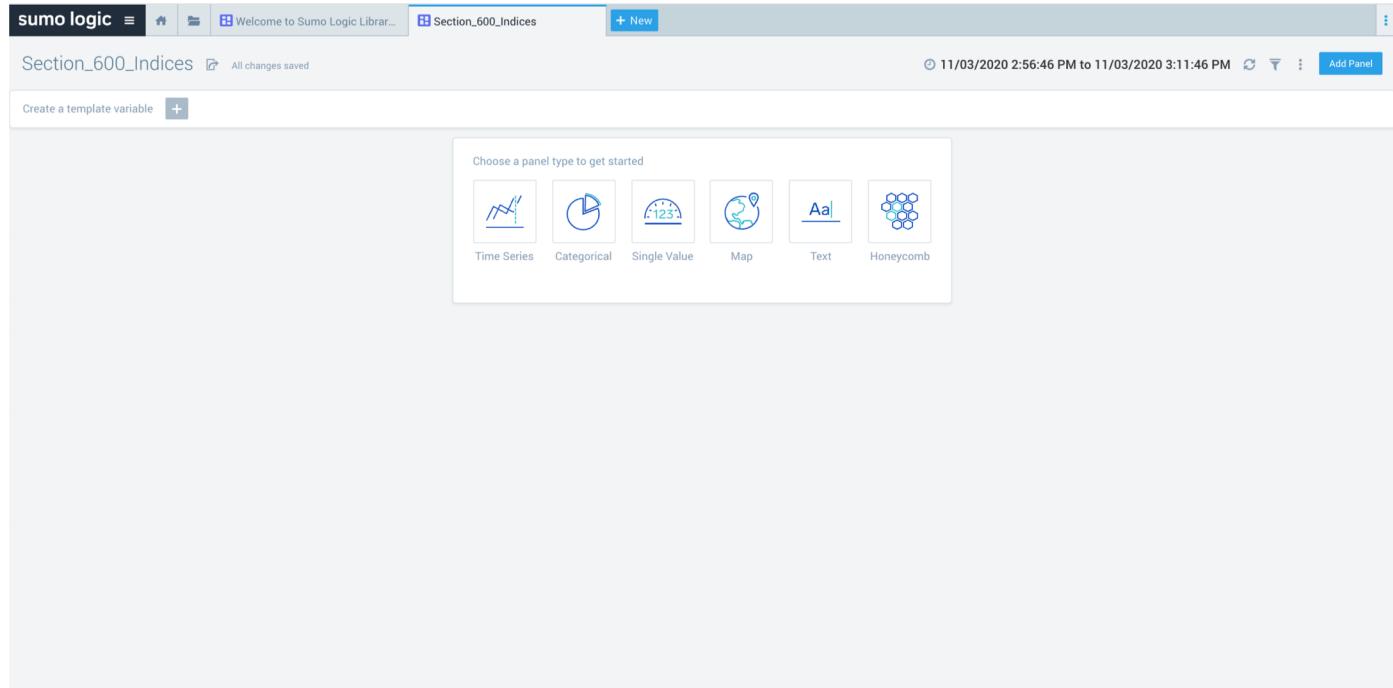
# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

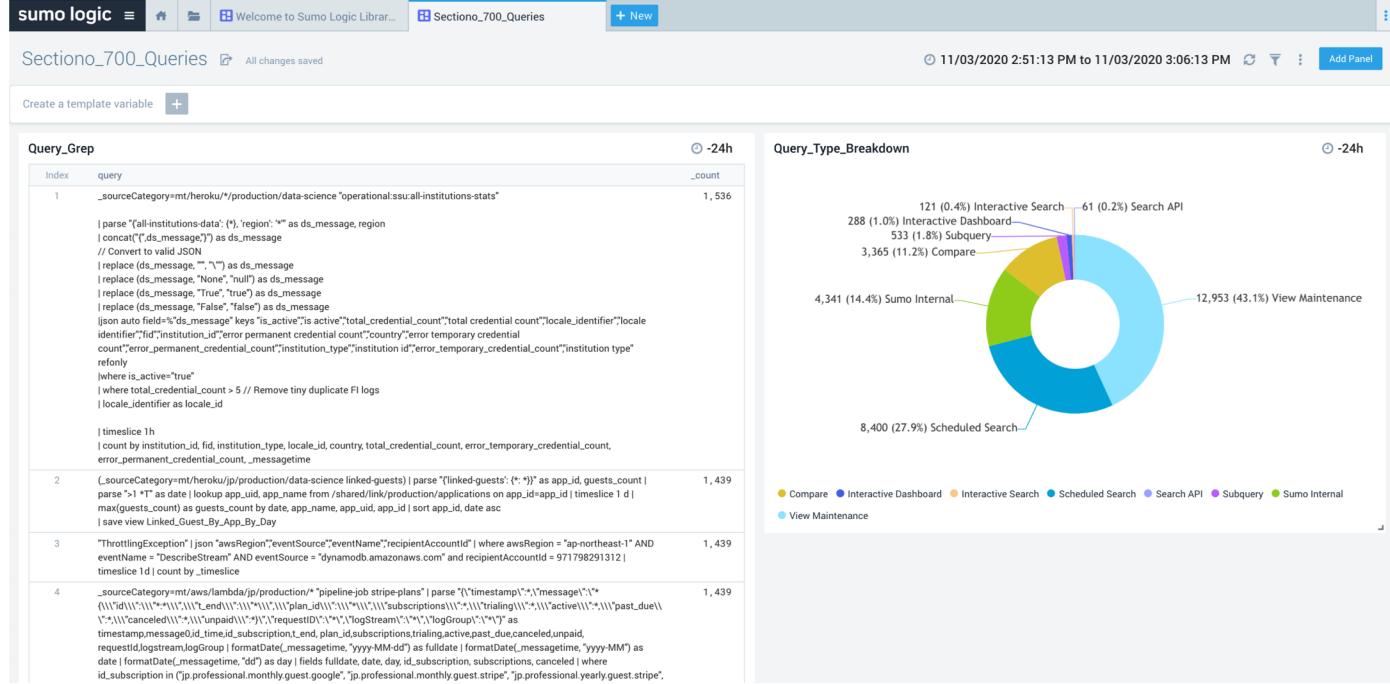
# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

# Sumo Logic Librarian

The screenshot shows the Sumo Logic Librarian interface with two main panels:

- Operator Documentation**: A table listing various operators with their corresponding doclinks:

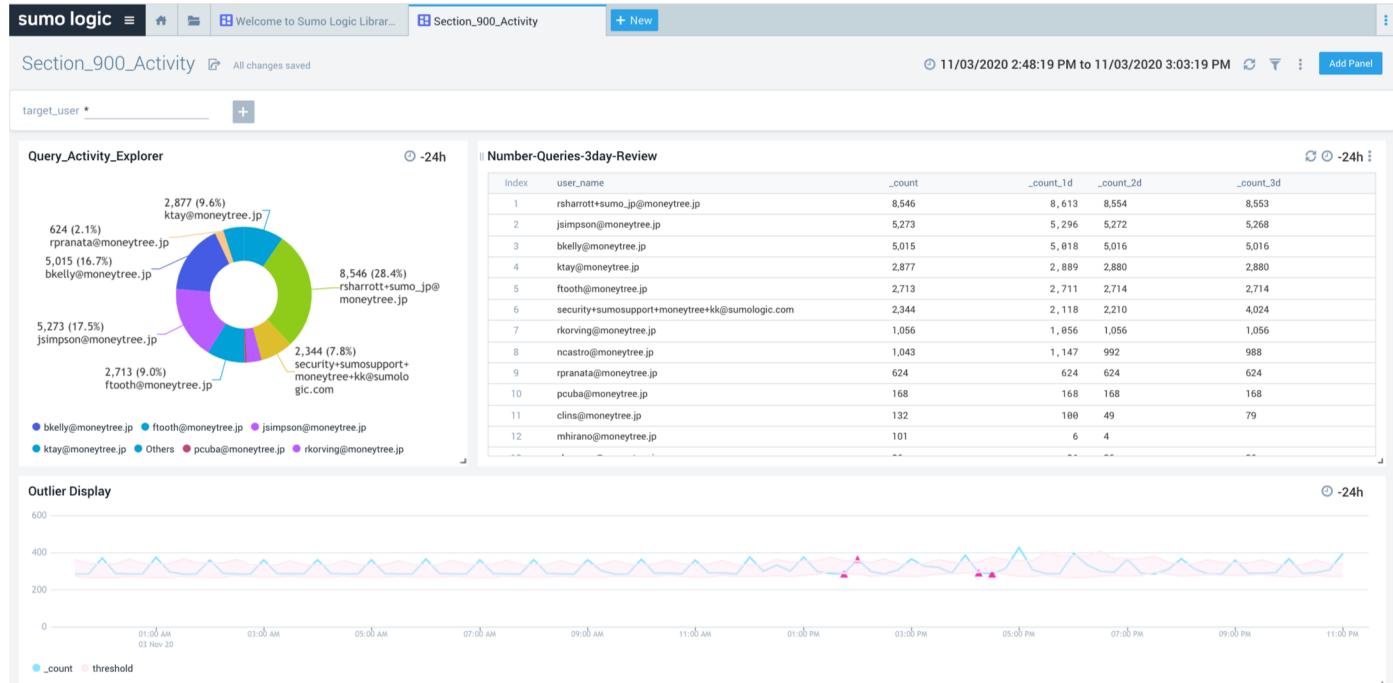
Index	doclink
1	Luhn
2	merge
3	tanh
4	ipv4ToNumber
5	tolower
6	standard-deviation
7	uridecode
8	now
9	log
10	hexToDec
11	limit
12	isEmpty
13	log10
14	timeslice
15	median
16	substring
17	parseHex
18	quantize
19	contains
20	min
21	expml
- Metavariable Documentation**: A table listing various metavariables with their corresponding doclinks:

Index	doclink
1	_sourcehost
2	_group
3	_approxcount
4	_collector
5	_X
6	_messagetime
7	_raw
8	_deltaPercentage
9	_count
10	_budget
11	_group_size
12	_sourcATEGORY
13	_cluster_id
14	_group_duration
15	_avg
16	_countViolation
17	_index
18	_min
19	_count_error

## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

# Sumo Logic Librarian



## Organized into Sections

- **Section-000 – Data Sources**
- **Section-100 - Partitions**
- **Section-200 - Source Categories**
- **Section-300 - Extraction Rules**
- **Section-400 - Saved Views**
- **Section-500 - Lookup Files**
- **Section-600 - Indices**
- **Section-700 - Queries**
- **Section-800 - Documentation**
- **Section-900 - Activity**

# Thank you

sumo logic

s u

**Continuous Intelligence  
Platform™**

m o