Become a

Sumo Generalist

Fundamentals Certification

sumo logic

Course Agenda

10 min.	Overview of Sumo logic
10 min.	Demo our monitoring and troubleshooting
10 min.	Hands-on Labs: View all collected data
30 min.	Search, parse, and analyze data
20 min.	Trending analysis and monitor critical events
30 min.	Creating and modifying dashboards & create an alert
60 min.	Get certified as a Sumo Generalist Fundamentals

Sumo Logic confidential

How can Sumo Logic help you today?

Continuous intelligence for modern apps

Operational Analytics

- Good user experience
- Better app performance
- Reduce MTTI/R

Security Analytics

- Secure cloud workloads
- Lower cost of compliance
- Compliant service

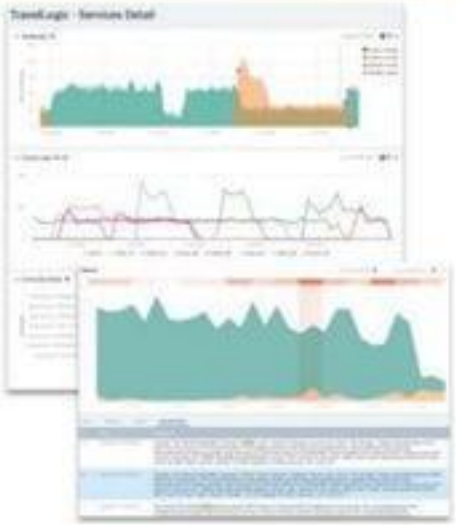
Business Analytics

- Faster time to market
- More competitive offering
- Improved customer support

Demo: Monitor and Troubleshoot

ALERTS
notify of a critical event

METRICS
to identify what's going on



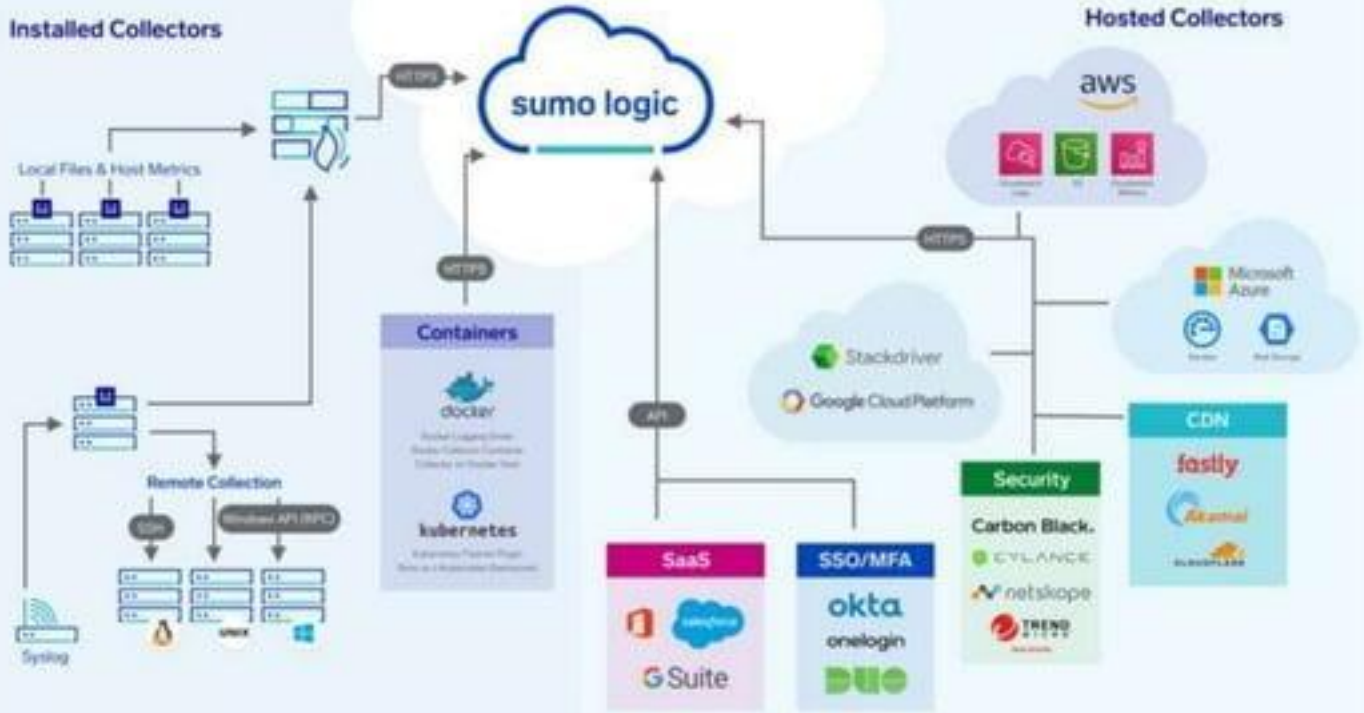
LOGS
to identify why it's happening

Sumo Logic confidential

1. How does Sumo Logic **help me**?

Demo & Dataflow

Sumo Logic Data Flow


Installed Collectors
Hosted Collectors
sumo logic
HTTPS
Local Files & Host Metrics
Containers
docker
kubernetes
Remote Collection
Syslog
aws
Microsoft Azure
Stackdriver
Google Cloud Platform
API
CDN
fastly
Security
Carbon Black.
CYLANCE
netskope
SaaS
G Suite
SSO/MFA
okta
onelogin
DUO

Sending Data ⇨ Metadata

Metadata tags are associated with each log message that is collected.

Tag	Description
`_collector`	Name of the collector (defaults to hostname)
`_sourceHost`	Hostname of the server (defaults to hostname)
`_sourceName`	Name and Path of the log file
`_source`	Name of the source this data came through
`_sourceCategory`	**Can be freely configured. Main metadata tag (e.g. labs/apache/access)**

Sumo Logic Confidential

Tutorial: Hands-on Exercises

Training Environment:

service.sumologic.com

username: training+labs@sumologic.com

password:

Hands-on Labs:

- Follow along using the labs found under **Home** > **Certifications** > TUTORIAL

Fundamentals Certification

In order to get credit for the exam, go to **your own instance**, and the to **Certification Tab**.

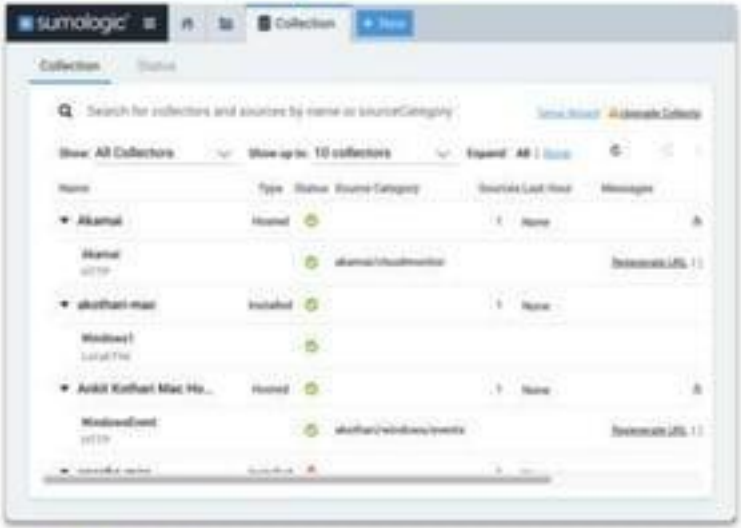
- Online Exam
- 30 Multiple choice questions
- 60-minute time limit
- 3 attempts

2. What data can I analyze?

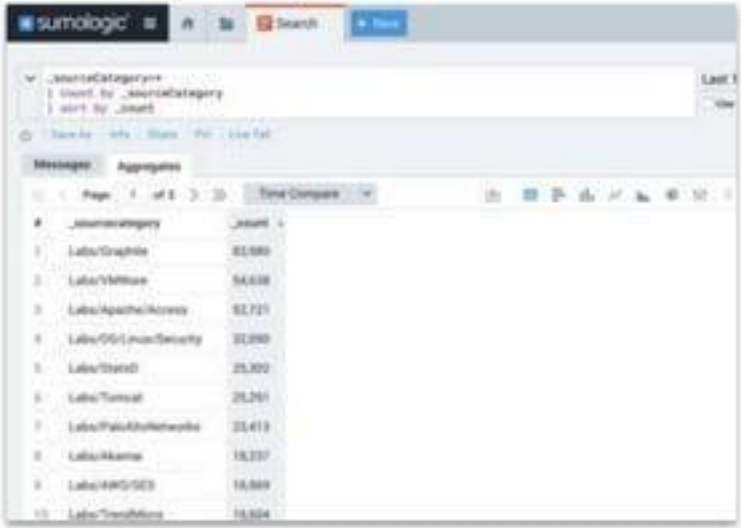
What's available to me?

What Data can I Analyze?

Option 1
Explore your Collectors



Option 2
Search for source categories



Sumo Logic Confidential

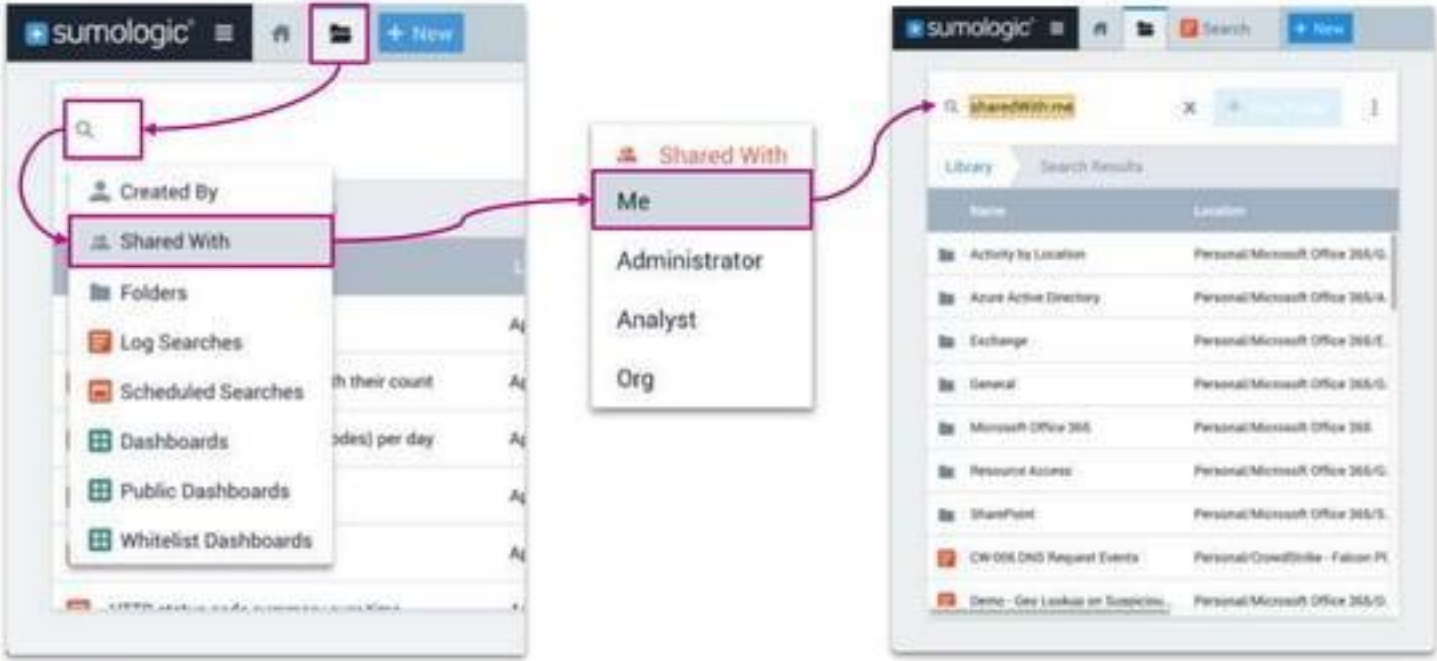
3. How can I analyze my data?

Search, Parse, Analyze

sumo logic

Data Analytics – Shared Content

Has someone already analyzed this same data?



Sumo Logic Confidential

Data Analytics – Sumo Logic Apps

Is there an App for it? Search in the **App Catalog** and Install it.

Hands-on Lab

Using Sumo Logic Tutorial

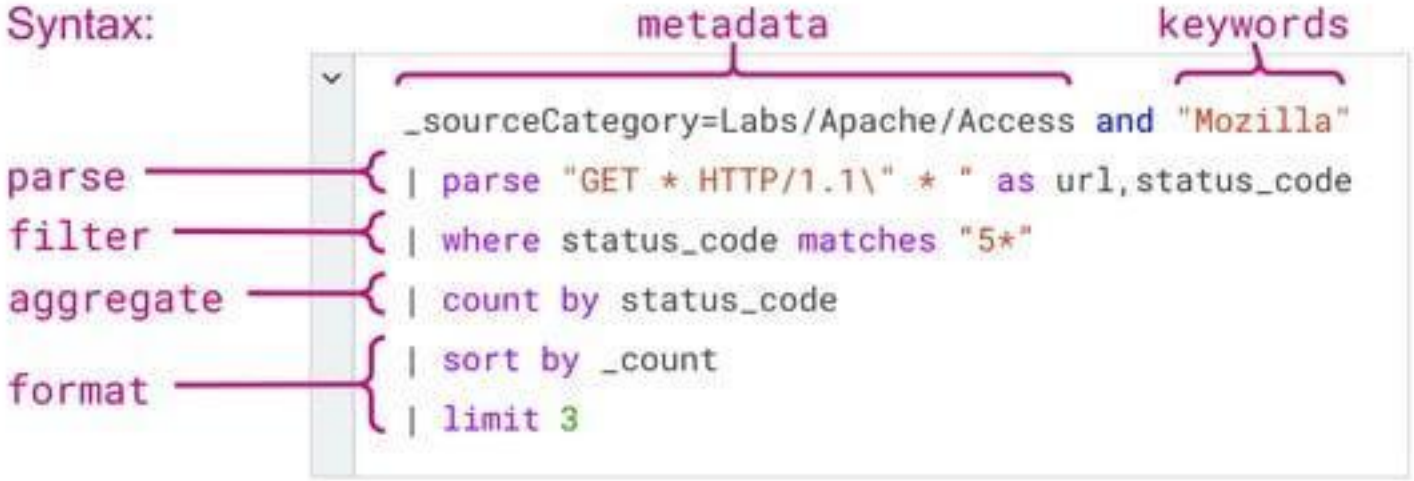
Complete Part 1: Viewing Data

- Sign in
- Identify data available
- Search for existing content from other users
- Install a Sumo Logic App

Sumo Logic Confidential

Data Analytics ⇨ Query Syntax

Keywords and operators, separated by pipes, that build on top of each other

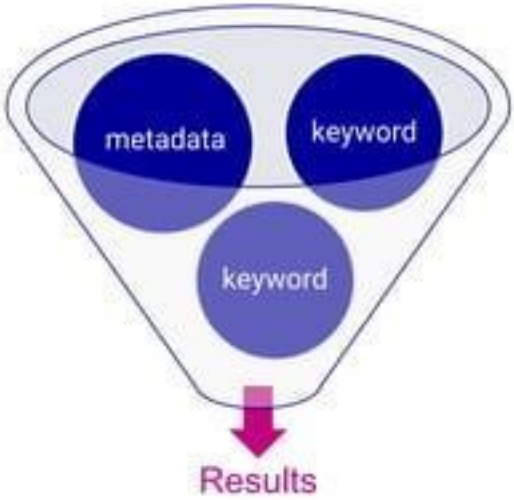


Data Analytics ⇨ Query Syntax

Use metadata and keywords to narrow your search scope

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```



Data Analytics ⇨ Query Syntax

Extract meaningful fields to provide structure to your data

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

Parse Anchor:

```
| parse " *@* " as user,domain
```

Parse Regex:

```
| parse regex "(?<src_ip>\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})"
```

Other Parse Operators:

```
csv, json, keyvalue, split, xml
```

Learn more: Parse Operators

Data Analytics ⇨ Query Syntax

Further filter results using your extracted fields

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

where operator:

```
| where !(status_code=304)
```

in operator:

```
| if(status_code in("501","502"),
"Error","OK") as code_type
```

Other Filter Operators:

```
join, lookup, matches, filter,
isEmpty, isNull, isBlank
```

Learn more: Filter operator example

Sumo Logic Confidential

Data Analytics ⇨ Query Syntax

Evaluate messages and place them into groups

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

count operator:

```
| count by status_code
```

avg operator:

```
| avg(size) by src_ip
```

pct operator:

```
| pct(filesize,75) by _sourceHost
```

Other Aggregation Operators:

```
sum, count_distinct, stddev, min, max
```

Learn more: Aggregation operators

Data Analytics ⇨ Query Syntax

Format to display desired results succinctly

Syntax:

```
metadata + keywords
| parse
| filter
| aggregate
| format
```

top operator:

```
| top 5 src_ip by avg_size
```

fields operator:

```
| fields src_ip, avg_size
```

transpose operator:

```
| transpose row src_ip column url
```

Other formatting Operators:

```
format, formatdate, limit, sort
```

Learn more: Trends over time using transpose

Advanced Analytics

Geo Lookup

```
_sourceCategory=Labs/Apache/Access
| lookup latitude, longitude from geo://default on ip=src_ip
| count by latitude, longitude
```

Outlier

```
_sourceCategory=Labs/Apache/Access and status_code=404
| timeslice 1m
| count(status_code) as error_count by _timeslice
| outlier error_count
```

Predict

```
_sourceCategory=Labs/Apache/Access
| timeslice 5m
| count as requests by _timeslice
| predict requests by 5m forecast=12
```

Advanced Analytics

LogReduce

Find the "needle in the haystack" by identifying patterns.

```
_sourceCategory=Labs/snort
| logreduce
```

LogCompare

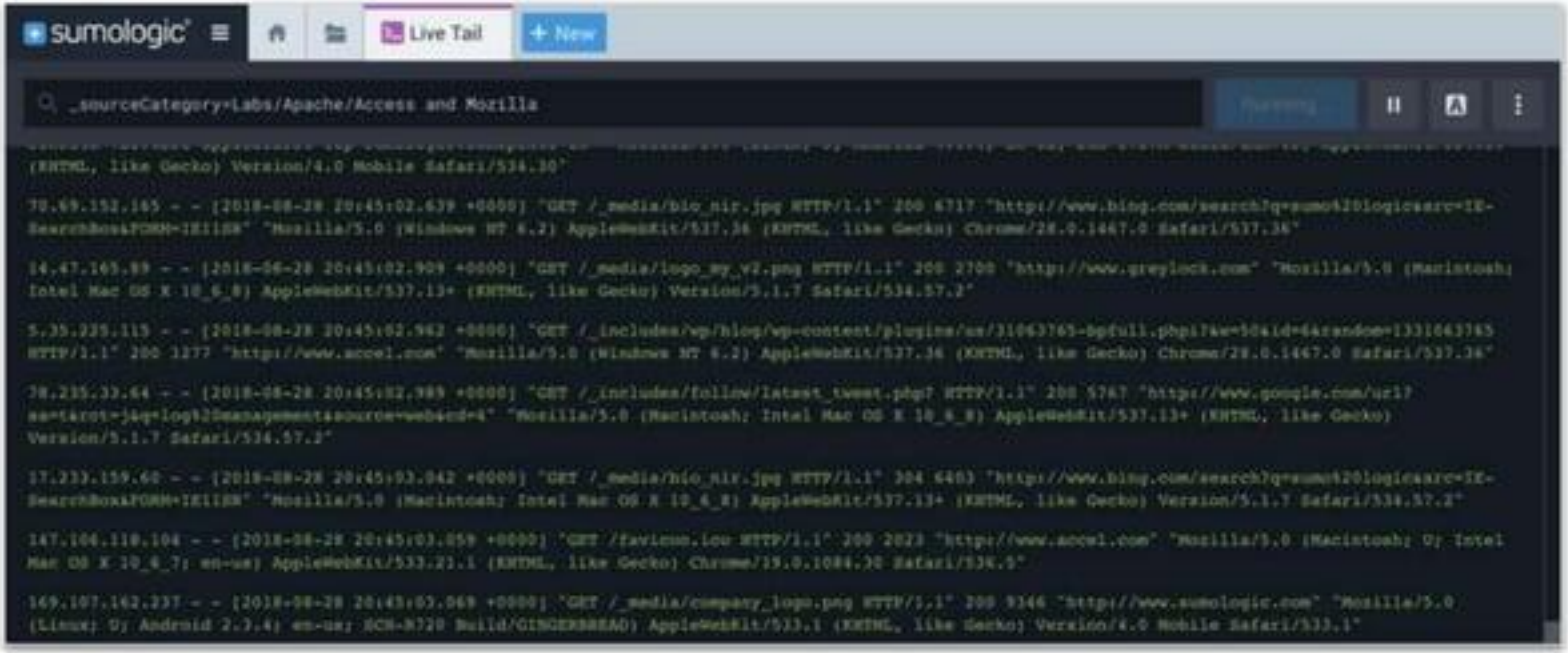
Compare today's patterns with patterns in the past.

```
_sourceCategory=Labs/snort
| logcompare -24h
```

Sumo Logic Confidential

Advanced Analytics

Get real time view of your logs with Live Tail



Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 2: Search for Log Data

- ➔ Search and Parse

Complete Part 3: Chart Your Data

- ➔ Aggregate
- ➔ Format
- ➔ Chart your data

Sumo Logic Confidential

4. How can I monitor my data?

Dashboards and Alerts

sumo logic

Monitoring - Dashboards

- Each **Panel** processes results from a single search
- **Drill down** into corresponding query or link to another Dashboard

- **Live Mode**: provides live stream of data

- Use Dashboards as templates with **Filters**

sumo logic

Sumo Logic Confidential

Let's take a 15 min break

Return promptly to play Kahoot
3 multiple choice questions

The highest score wins a prize!

Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 4: Create and Share a Dashboard

- ➔ Create a Dashboard
- ➔ Change the Theme
- ➔ Share with your Organization

Complete Part 5: Modify a Dashboard

- ➔ Modify the query of an existing Dashboard Panel

Sumo Logic Confidential

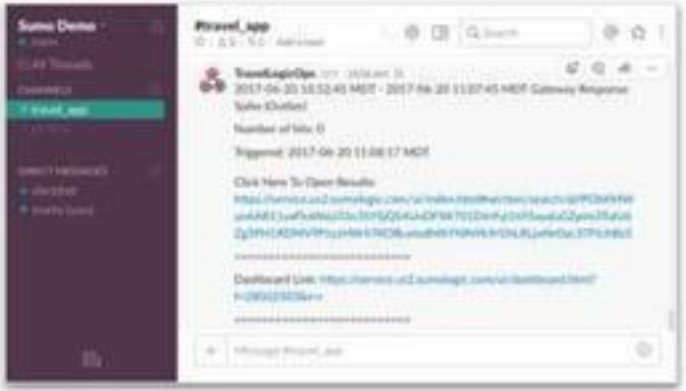
Monitoring - Alerts

Scheduled Searches trigger Alerts when a condition is met.

Alert Types:

- Email
- Webhook
- Save to Index
- Script Action

➢ Learn More: 2 Key Principles for Creating Meaningful Alerts



Hands-On Labs

Using Sumo Logic Tutorial

Complete Part 6: Create an Alert

- ➔ Schedule and test an Alert
- ➔ Delete Alert after testing

Sumo Logic Confidential

Metrics

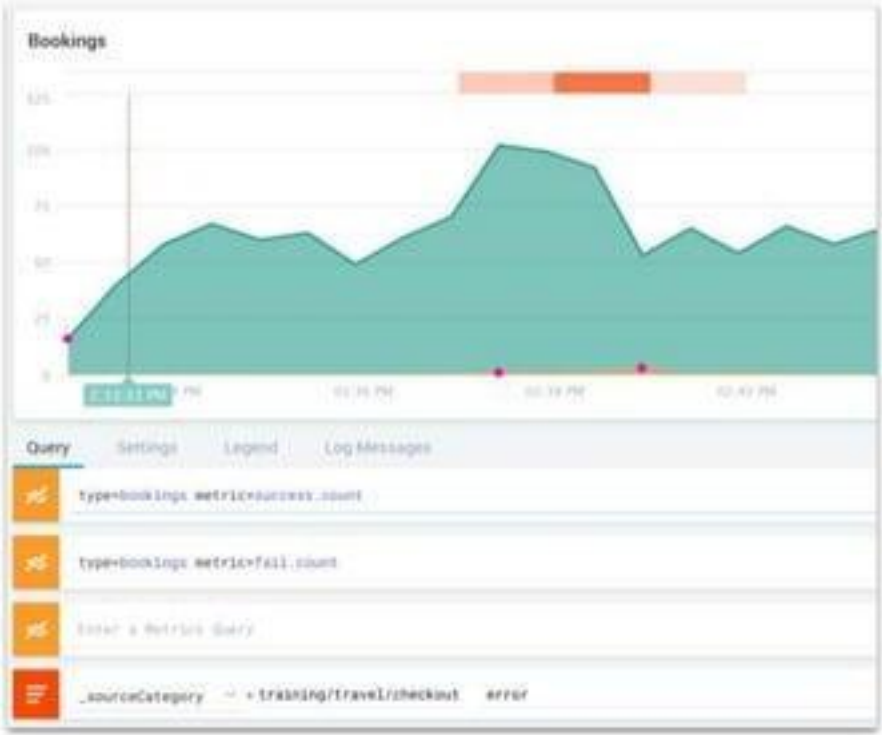
Sources, Dashboards and Alerts

sumo logic

Logs and Metrics - Overlay

Overlay helps you correlate metrics to the relevant logs.

- Metrics identify the **what**.
- Logs help identify **why**.



Sumo Logic Confidential

Ingesting Metrics

Host Metrics

AWS ECS

✓ **Learn More:**
Setting up Host Metrics

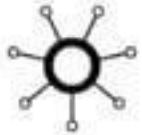
AWS Metrics

AWS CloudWatch Metrics

✓ **Learn More:**
Setting up AWS Metrics

Graphite-Compatible

Telegraf



CollectD

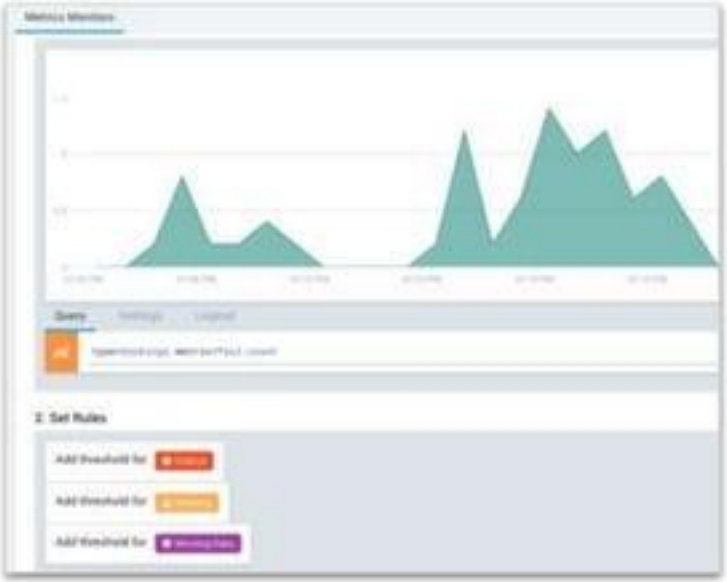
Dropwizard

StatsD

✓ **Learn More:**
Setting up Graphite Metrics

Metrics - Dashboards and Alerts

Dashboards can contain Metrics and Logs Panels

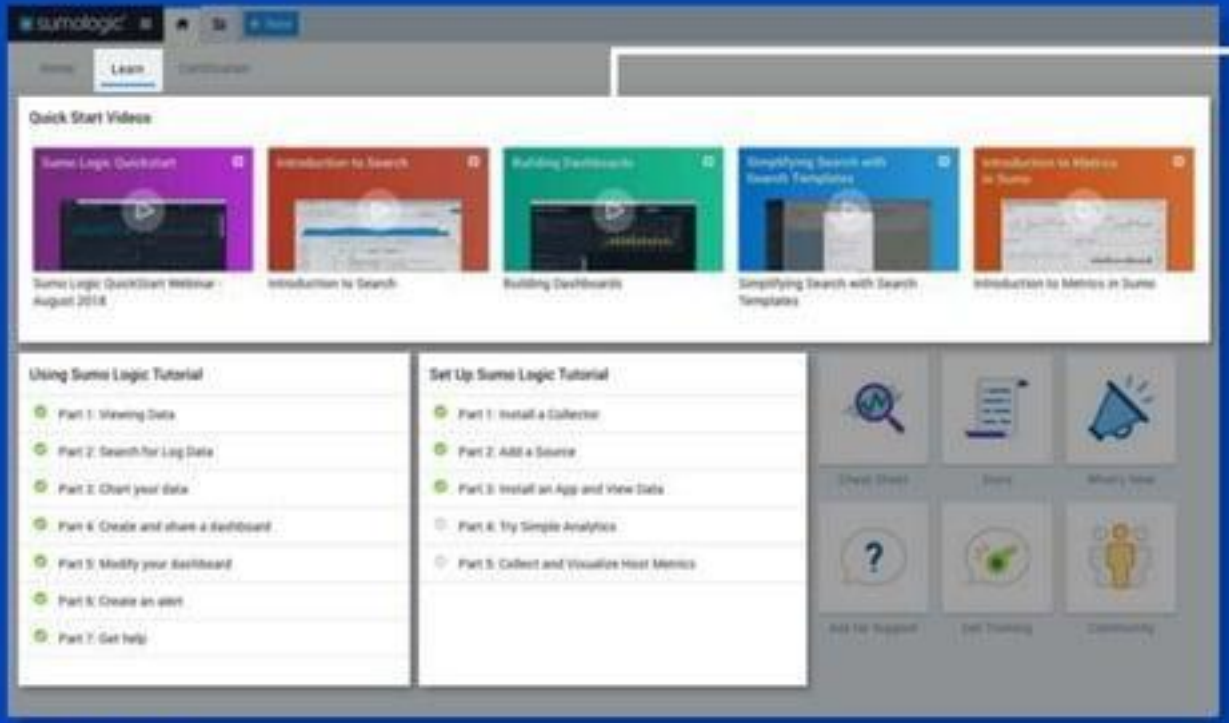


Metric Monitors alert on thresholds (Critical, Warning, Missing Data)

5. Where do I go from here?

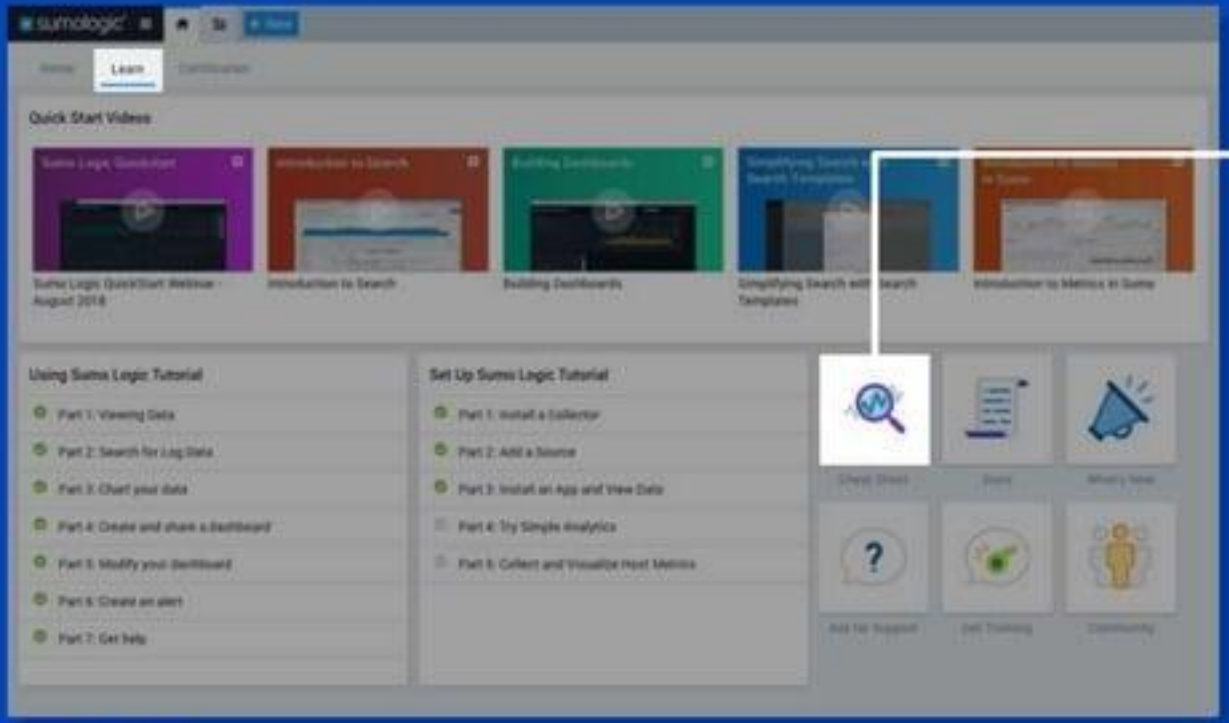
Training, Docs, Community, Support

Need knowledge? ⇨ try the **Learn** tab



Explore the tutorials

Need knowledge? ⇨ try the **Learn** tab

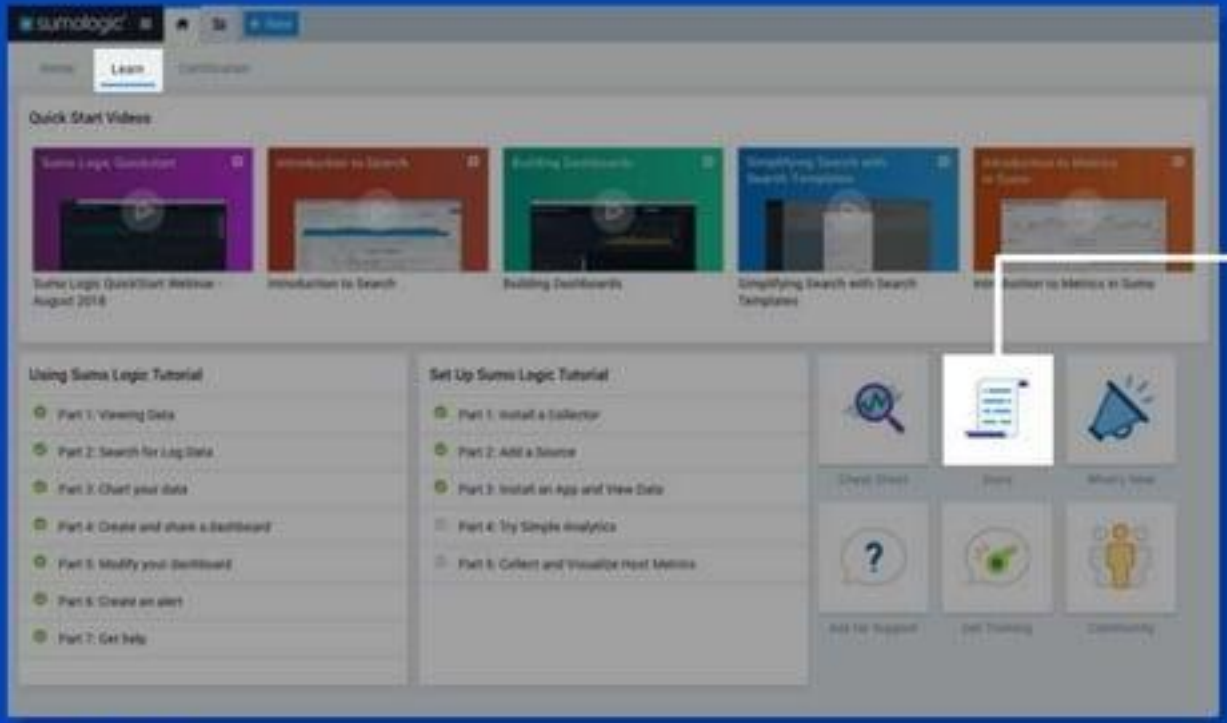


Explore the tutorials

Access comprehensive lists of operators and more

Sumo Logic Confidential

Need knowledge? ⇨ try the **Learn** tab



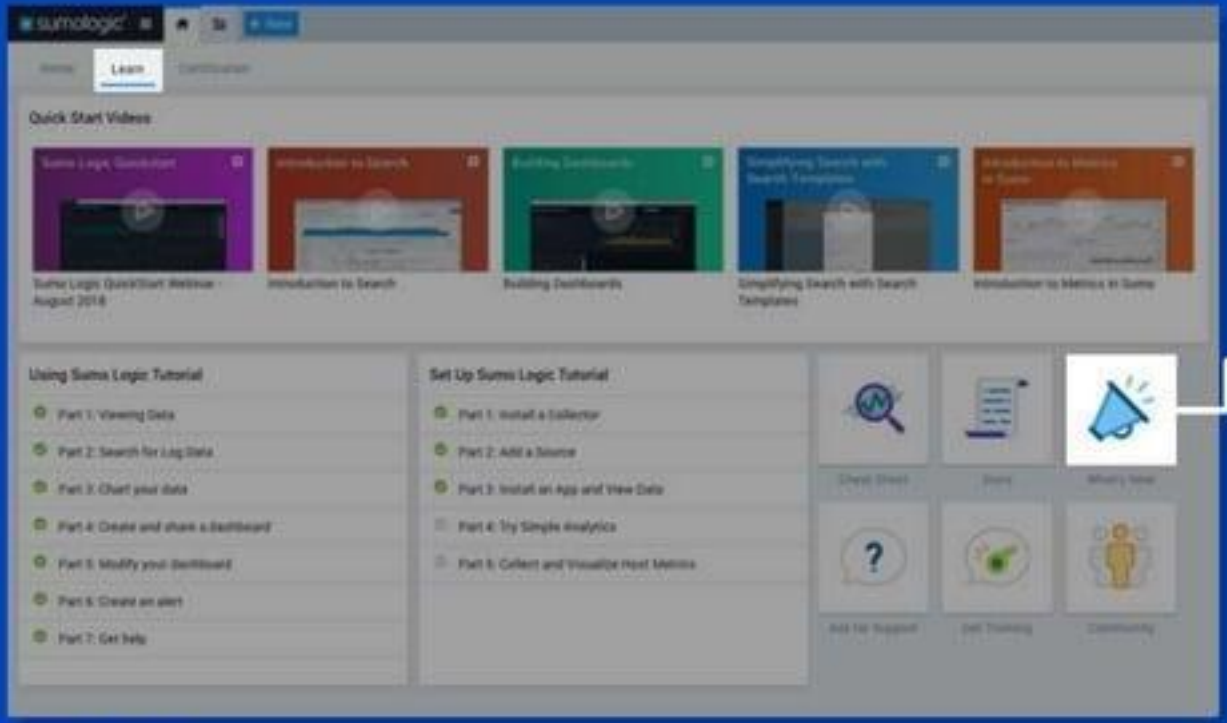
Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Sumo Logic Confidential

Need knowledge? ⇨ try the **Learn** tab



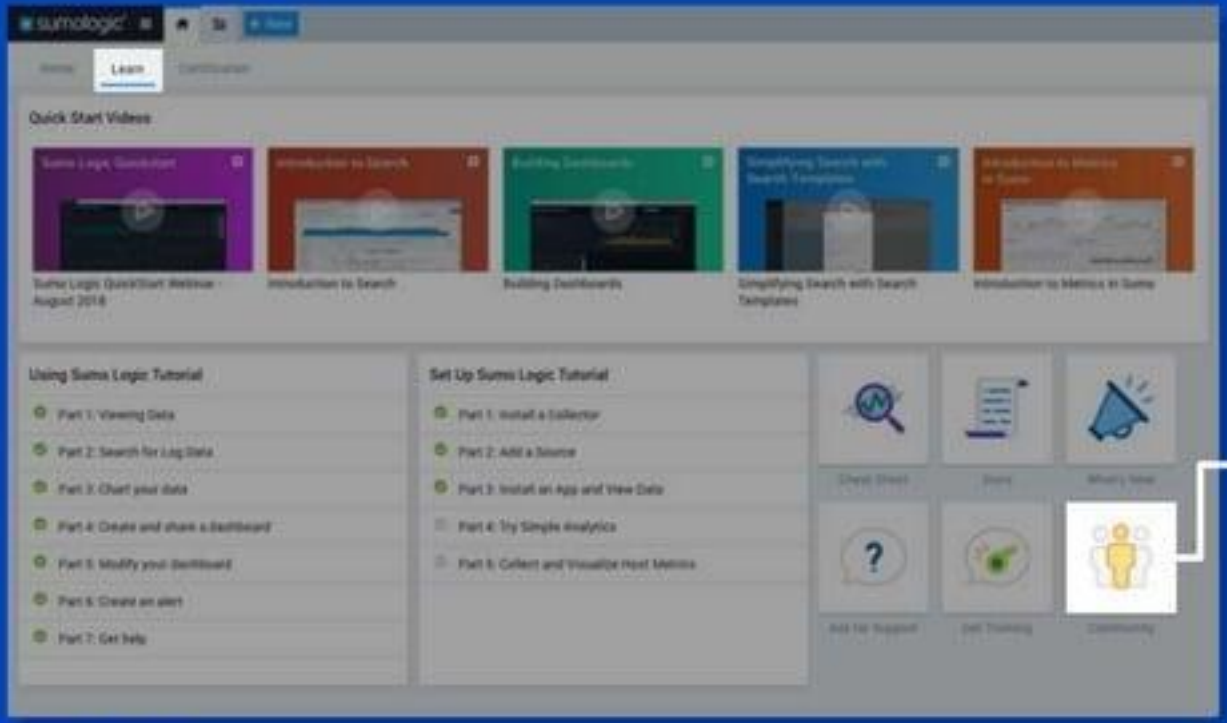
Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Need knowledge? ⇨ try the **Learn** tab



Explore the tutorials

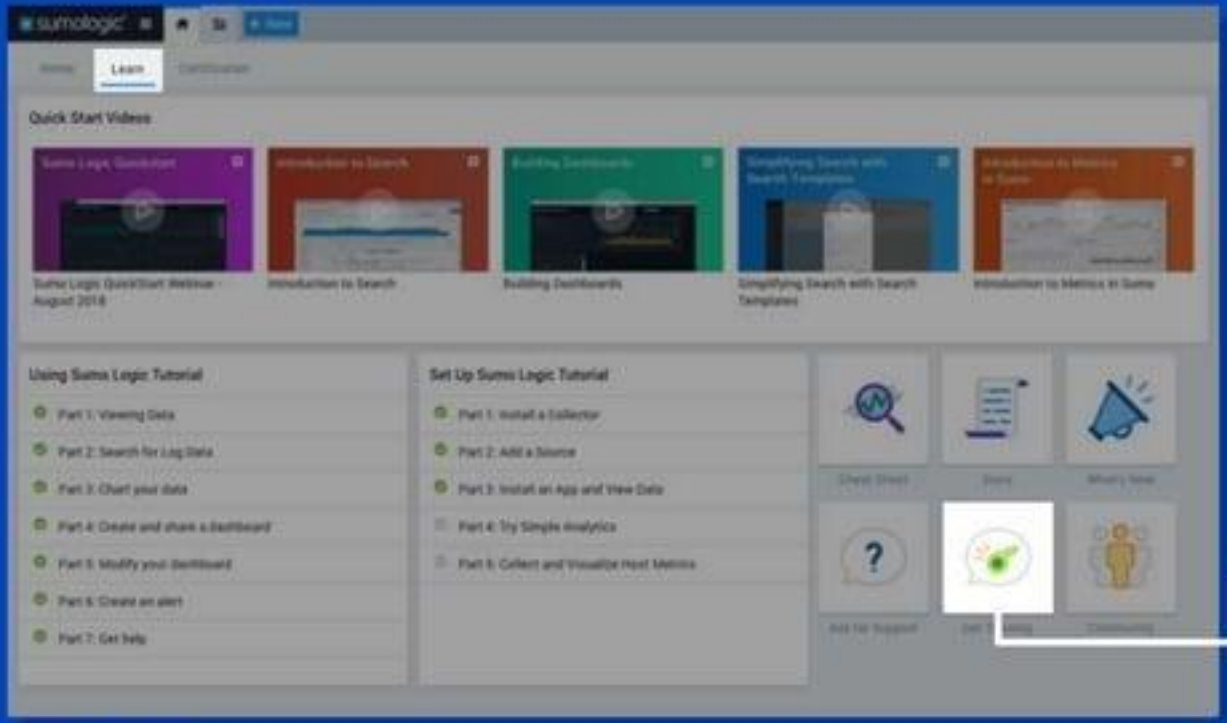
Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Need knowledge? ⇨ try the **Learn** tab



Explore the tutorials

Access comprehensive lists of operators and more

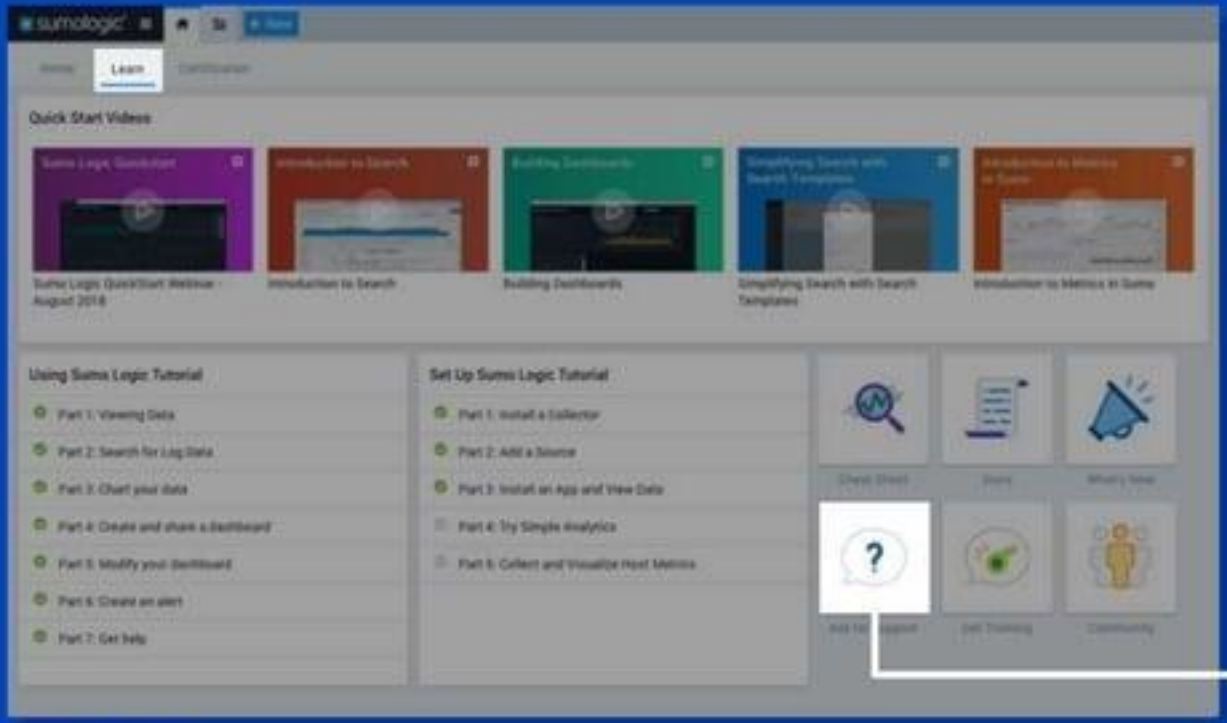
Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Need knowledge? ⇨ try the **Learn** tab



Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

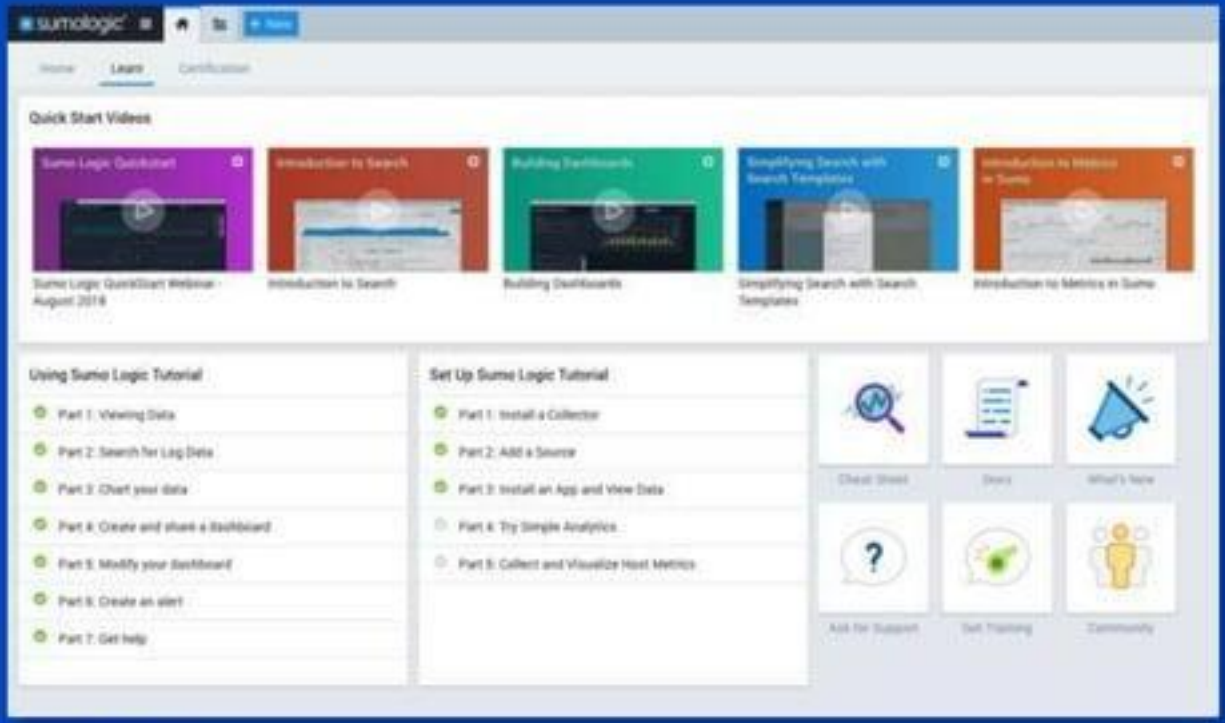
Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

Need knowledge? ⇨ try the **Learn** tab



Explore the tutorials

Access comprehensive lists of operators and more

Every feature and tool covered in docs

Find out What's New

Find answers or post your questions to Community

Attend/review training and get certified

Open a Support case

Questions?

In order to get credit for the exam,

In YOUR OWN INSTANCE, go to Certification Tab.

- Online Exam
- 30 Multiple choice questions
- 60-minute time limit
- 3 attempts
- sumologic.talentlms.com

Sumo Logic Confidential

Sumo Logic Certification

- Make sure to log out of the training account you were using and sign in with your own account
- If you do not have a working login, go to sumologic.talentlms.com to sign up for an account

If you find your login is cycling back to the exam screen, do the following:

- Click on Help in the black left bar
- Click Community in the black left bar
- An email verification should be sent
- Once you verify, you should able to take the exam without any issues

For passing the exam, you will earn:

- SWAG
- A Certificate
- An invitation to our LinkedIn Group
- The respect of your peers
- Fame, Fortune and more...

How did we do?

Please take our survey:
https://forms.gle/2KMtxPuD9cSYV8SJ6

s u

Empowering the people who power modern business

m o

sumo logic

s u

Empowering the people who power modern business

m o

sumo logic