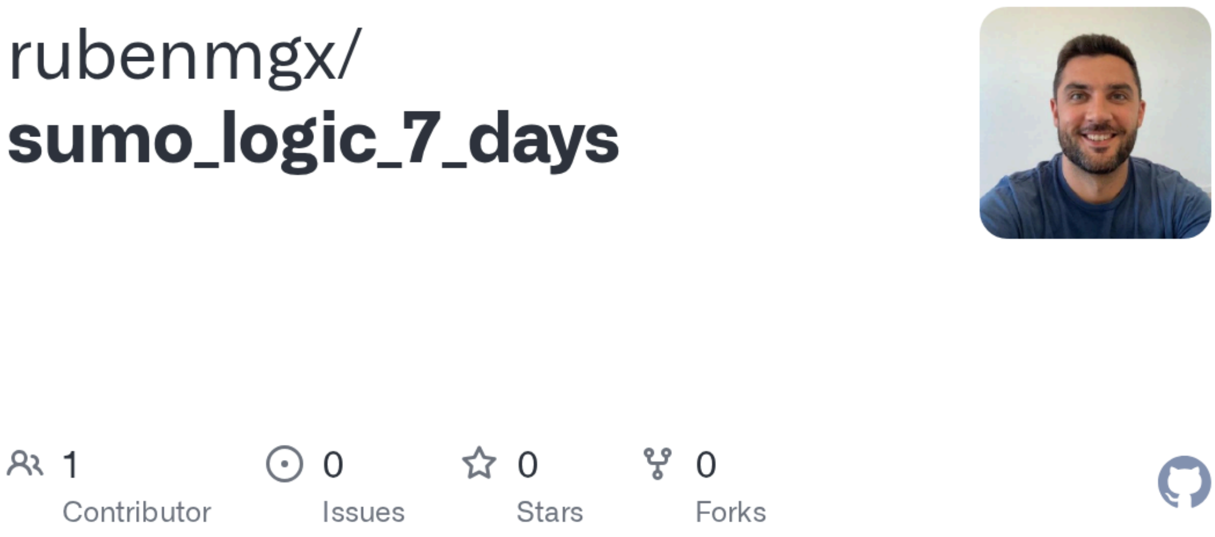
rubenmgx/sumo_logic_7_days

github.com/rubenmgx/sumo_logic_7_days



rubenmgx/
sumo_logic_7_days

Name	Last commit message	Last commit date
rubenmgx Update README.md 2c27571 · 5 months agoJul 28, 2025		
README.md	Update README.md	5 months agoJul 28, 2025

Repository files navigation

Sumo Logic 7-Day Learning Roadmap: From 0 to 100

This roadmap is designed to guide you through learning Sumo Logic in 7 days, from foundational concepts to advanced features. It emphasizes hands-on practice and leveraging Sumo Logic's official resources.

Crucial First Steps:

- **Sumo Logic Free Trial:** Sign up for a free trial to perform all hands-on exercises.
  Link: Sumo Logic Free Trial
- **Sumo Logic Learning Portal:** This portal offers self-paced e-learning modules with videos and guided labs. Access it from your Sumo Logic Home page (`Learn` or `Get Certified` tab).
  Link (General Learning Portal): Sumo Logic Training
- **Sumo Logic Official Documentation:** Your comprehensive guide for all features, detailed instructions, and examples.
  Link: Sumo Logic Docs

Day 1: Introduction to Sumo Logic & Data Ingestion Fundamentals

Morning: Sumo Logic Overview & UI Tour

- **Goal:** Understand what Sumo Logic is, navigate the UI.
- **Resources:**
  - **Doc:** What is Sumo Logic?
  - **Doc:** Getting Started with Sumo Logic
  - **Video:** Search for "Sumo Logic UI Tour" or "Introduction to Sumo Logic" on the Sumo Logic YouTube channel.
- **Testing/Practice:**
  - **Activity 1:** Log into your Sumo Logic trial. Navigate to the Home page, then explore the "Search," "Dashboards," and "Metrics" tabs. Spend 10 minutes clicking around to get a feel for the interface.
  - **Activity 2:** Locate the "App Catalog" (usually under "Manage Data" or "Library"). Browse through some of the pre-built apps to see what's available.

Afternoon: First Data Ingestion & Basic Search

- **Goal:** Successfully ingest data and perform basic searches using metadata and keywords.
- **Resources:**
  - **Doc (Installed Collector - Local File):** Collect Local Files
  - **Doc (Hosted Collector - AWS CloudTrail):** Collect AWS CloudTrail Logs (Optional, if you have an AWS account).
  - **Doc (Basic Search Operators):** Basic Search Operators

- **Testing/Practice:**
  - **Activity 1 (Hands-on Ingestion):**
    1. Install an **Installed Collector** on your local machine (or a VM).
    2. Configure a **Local File Source** to ingest a simple log file (e.g., your web server access logs, or create a simple `test.log` file with a few lines of text like "INFO: Application started", "ERROR: Connection failed", "User 'admin' logged in").
    3. Verify the collector and source status in the Sumo Logic UI.
  - **Activity 2 (Basic Search):**
    1. Go to the "Search" page.
    2. Search for `_sourceCategory="your/category"` (replace `your/category` with what you set for your local file source). Verify your logs appear.
    3. Search for a specific keyword from your log file (e.g., `"ERROR"` or `"logged in"`).
    4. Change the time range to "Last 15 minutes" or "Last 60 minutes" to see how it affects results.
    5. **Challenge:** Find all lines in your logs that contain both "User" and "logged in".

Day 2: Core Log Search & Analysis

Morning: Parsing and Field Extraction

- **Goal:** Understand how to extract meaningful fields from unstructured logs.
- **Resources:**
  - **Doc (`| parse` operator):** Parse Operator
  - **Doc (Field Extraction Rules - FERs):** Create a Field Extraction Rule
  - **Video:** Search for "Sumo Logic Field Extraction Rules" on YouTube / Sumo Logic channel.
- **Testing/Practice:**
  - **Activity 1 (Using `| parse`):**
    1. Take a raw log line from your ingested data that contains some structured information (e.g., `[INFO] user=john message="login success" ip=192.168.1.1`).
    2. In a search, pipe this log to `| parse "user=* message=\"*\" ip=*" as user, message, ip`.
    3. Verify that `user`, `message`, and `ip` fields are extracted and appear in the "Fields" sidebar.
  - **Activity 2 (Creating an FER):**
    1. Identify a common pattern in your ingested logs that needs parsing.
    2. Go to **Manage Data > Settings > Field Extraction Rules**.
    3. Create a new FER based on the log pattern from Activity 1. Test it in the FER editor to ensure it extracts the fields correctly.
    4. Run a new search for logs that should be parsed by your FER. Verify the fields are now automatically available.

Afternoon: Basic Aggregations & Grouping

- **Goal:** Perform basic statistical analysis and group your log data.
- **Resources:**
    - **Doc (Aggregate Operators):** Aggregate Operators (Focus on `count`, `sum`, `avg`, `min`, `max`, `by`.)
    - **Doc (`| timeslice`):** Timeslice Operator
    - **Doc (`| top`, `| rare`):** Top Operator & Rare Operator
- **Testing/Practice:**
    - **Activity 1 (Counting and Grouping):**
        1. Search for all `ERROR` logs. Then, pipe the results to `| count by _sourceHost`. What are your top 3 hosts with errors?
        2. If you have an `ip` field (from parsing), run: `| count by ip | top 5 ip`. Identify the top 5 IPs.
    - **Activity 2 (Time-based Aggregation):**
        1. Run a search like: `_sourceCategory="your/category" | timeslice 1h | count by _timeslice`.
        2. Change the visualization to a "Column Chart." Observe the distribution of logs over time.
        3. **Challenge:** Modify the query to count "ERROR" messages per hour: `_sourceCategory="your/category" "ERROR" | timeslice 1h | count by _timeslice`.

Day 3: Visualizations & Dashboards

Morning: Creating Compelling Visualizations

- **Goal:** Convert raw data into various chart types and understand LogReduce/LogCompare.
- **Resources:**
    - **Doc:** Create a Dashboard
    - **Doc:** Dashboard Panel Types
    - **Doc (LogReduce/LogCompare):** LogReduce & LogCompare
    - **Video:** Analytics with LogReduce and LogCompare

- **Testing/Practice:**
  - **Activity 1 (Chart Types):**
    1. Run the query `_sourceCategory="your/category" | count by _sourceHost`.
    2. Experiment with different chart types (Bar, Pie, Table) from the visualization options. Which one best represents the data?
  - **Activity 2 (LogReduce/LogCompare):**
    1. Run a broad search for a log category with varied messages.
    2. Click "LogReduce" in the search results. Analyze the identified patterns. What commonalities do you see?
    3. Try "LogCompare" to compare log patterns from two different time ranges (e.g., last 1 hour vs. previous hour).

Afternoon: Building and Customizing Dashboards

- **Goal:** Assemble saved searches into interactive dashboards and explore pre-built apps.
- **Resources:**
  - **Doc:** Add Panels to a Dashboard
  - **Doc:** Dashboard Filters
  - **Doc:** Sumo Logic App Catalog
- **Testing/Practice:**
  - **Activity 1 (Custom Dashboard):**
    1. Save at least three of your searches from Day 2 (e.g., error count by host, login successes, top IPs).
    2. Go to **New > Dashboard**. Create a new dashboard.
    3. Add panels using your saved searches. Arrange them on the dashboard.
    4. Add a **dashboard filter** for `_sourceHost` (if applicable) and see how it affects your panels.
  - **Activity 2 (App Catalog):**
    1. Browse the App Catalog. If you have any relevant data (e.g., AWS, Linux), install a corresponding app.
    2. Explore the pre-built dashboards provided by the app. How are they structured? What insights do they provide immediately?

Day 4: Advanced Search & Security Fundamentals

Morning: Advanced SPL & Query Optimization

- **Goal:** Use more complex SPL operators for refined analysis.

- **Resources:**
    - **Doc (`| where`, `if`, `case`):** Where Operator & If and Case Operators
    - **Doc (`| join`):** Join Operator
    - **Doc (Subqueries):** Subqueries
    - **Doc (Regex Operations):** Extract Operator
- **Testing/Practice:**
    - **Activity 1 (Conditional Logic):**
        1. Write a search that identifies logs where a `status_code` field (if you have one) is greater than or equal to `400` *and* the message contains "failed".
        2. Use `| if` to categorize events: `... | if (error_code = "404", "Page Not Found", "Other Error") as error_type | count by error_type`.
    - **Activity 2 (Subqueries/Join - Conceptual/Simple):**

        Conceptual: Imagine you have two log types: `_sourceCategory=webserver` (with `user_id`) and `_sourceCategory=auth_logs` (with `user_id` and `successful_login`). How would you find web server activity for users who had *failed* logins? (Think about a `| join` or subquery approach, even if you don't have this exact data).

Afternoon: Introduction to Security Monitoring

- **Goal:** Understand basic security use cases and how to set up alerts.
- **Resources:**
    - **Doc (Security Use Cases):** Security Use Cases
    - **Doc (Scheduled Searches & Alerts):** Create a Scheduled Search
- **Testing/Practice:**

    Activity 1 (Security Alert Simulation):

    1. Create a log entry in your local file source that simulates a security event, e.g., `"FAILED_LOGIN from IP 1.2.3.4 for user hacker"`.
    2. Write a search to detect this pattern (e.g., `_sourceCategory="your/category" "FAILED_LOGIN"`).
    3. Save this search.
    4. Configure a **Scheduled Search** based on this saved search. Set it to run every 5 minutes and trigger an email alert if results are found. Test the alert by adding another "FAILED_LOGIN" entry to your log file.

Day 5: Metrics & Observability Deep Dive

Morning: Metrics Ingestion & Metrics Explorer

- **Goal:** Get metrics into Sumo Logic and query them.

- **Resources:**
    - **Doc (Logs vs. Metrics):** Logs, Metrics, and Traces
    - **Doc (OpenTelemetry Collector):** Sumo Logic Distribution for OpenTelemetry Collector
    - **Doc (Metrics Explorer):** Metrics Explorer
    - **Video:** Search for "Sumo Logic Metrics Explorer Tutorial" on YouTube / Sumo Logic channel.
- **Testing/Practice:**
    - **Activity 1 (Metrics Ingestion):**
        1. Set up the Sumo Logic Distribution for OpenTelemetry Collector on your local machine.
        2. Configure it to collect basic host metrics (CPU, Memory, Disk I/O).
        3. Verify that metrics are being ingested by navigating to the "Metrics" tab in Sumo Logic.
    - **Activity 2 (Metrics Explorer):**
        1. In Metrics Explorer, search for a metric like `cpu_usage_total` or `memory_usage_bytes`.
        2. Experiment with different aggregations (e.g., `avg`, `max`) and grouping by dimensions (if any are available).
        3. Change the time range and visualization type (e.g., Line Chart).

Afternoon: Metrics Dashboards & Alerts

- **Goal:** Build metrics dashboards and configure metric-based alerts.
- **Resources:**
    - **Doc:** Create a Metrics Dashboard
    - **Doc (Metrics Monitors):** Create a New Monitor (for Metrics)
    - **Video:** Search for "Sumo Logic Metrics Alerts" or "Sumo Logic Monitors" on YouTube / Sumo Logic channel.
- **Testing/Practice:**
    - **Activity 1 (Metrics Dashboard):**
        1. Create a new Dashboard.
        2. Add panels displaying your ingested CPU and Memory metrics.
        3. Include multiple panels with different visualizations (e.g., average CPU as a line chart, current free memory as a single value).
    - **Activity 2 (Metrics Alert):**
        1. Create a **Monitor** (alert) for your CPU usage.
        2. Set a simple threshold (e.g., alert if `cpu_usage_total` > 80% for 5 minutes).
        3. If possible, simulate high CPU usage on your machine to trigger the alert and verify the notification.

Day 6: Cloud SIEM (Security Information and Event Management)

Morning: Cloud SIEM Architecture & Basics

- **Goal:** Understand core Cloud SIEM concepts.
- **Resources:**
  - **Doc:** What is Cloud SIEM?
  - **Doc:** Records, Signals, Entities, and Insights
  - **Video:** Cloud SIEM Overview
  - **Video:** Micro Lesson: How are Insights Generated in Cloud SIEM?
- **Testing/Practice (Conceptual/Exploration):**
  - **Activity 1:** Navigate to the "Security" tab in Sumo Logic. Explore the "Insights," "Signals," and "Entities" pages.
  - **Activity 2:** If your trial has sample Cloud SIEM data, review a few existing Insights. Click on an Insight to see the correlated signals and underlying records. How do different signals contribute to an Insight?

Afternoon: Threat Detection & Incident Response

- **Goal:** Get hands-on with security rules and investigating incidents.
- **Resources:**
  - **Doc:** About Cloud SIEM Rules
  - **Doc:** Write a Threshold Rule
  - **Video:** Search for "Sumo Logic Cloud SIEM Custom Rules" or "Sumo Logic Write a Rule" on YouTube / Sumo Logic channel.
- **Testing/Practice (Requires some SIEM data, even sample):**
  - **Activity 1 (Rule Exploration):**
    1. Go to **Cloud SIEM > Rules**. Browse through some of the pre-built rules.
    2. Select a simple rule (e.g., "Multiple Failed Logins"). Understand its logic: what conditions trigger it?
  - **Activity 2 (Simulated Custom Rule):**
    1. Imagine a log like `_sourceCategory=firewall "DROP access from suspicious_ip"` where `suspicious_ip` is a specific IP.
    2. Attempt to create a **Custom Rule** in Cloud SIEM that would generate a signal when this specific log appears. (You might not have live data for this, but practice the rule creation interface.)
    3. **Challenge:** If your trial has Cloud SIEM capabilities and you can ingest security logs (e.g., Windows Events, CloudTrail), try to create a simple log entry and a corresponding rule to generate a signal, then an insight.

Day 7: Administration, Automation & Advanced Topics

Morning: Administration & Account Management

- **Goal:** Understand how to manage your Sumo Logic environment.
- **Resources:**
  - **Doc:** Create and Manage Users
  - **Doc:** Manage Ingest Budgets
  - **Doc:** Manage Data Retention
- **Testing/Practice:**
  - **Activity 1 (User/Role Management):**
    1. Go to **Administration > Users and Roles**.
    2. Create a new user (e.g., "test_analyst") and assign them the "Viewer" role. Log in as this new user in a different browser/incognito window to see what they can access. (Then log out and delete this test user.)
  - **Activity 2 (Ingest Budgets/Retention - Conceptual):**
    1. Go to **Administration > Account > Ingest Budgets**. Understand how ingest budgets work. (You won't create one unless necessary for your trial.)
    2. Go to **Administration > Account > Data Management > Partitions**. See if any default partitions are set up and understand their purpose for data organization and retention.

Afternoon: Automation, APIs & Certification Prep

- **Goal:** Explore automation options and plan future learning.
- **Resources:**
  - **Doc (Sumo Logic API General):** Sumo Logic API Documentation (General)
  - **Doc (Access Keys):** Access Keys
  - **Link:** Sumo Logic Certifications Overview
- **Testing/Practice:**
  - **Activity 1 (API Exploration - Conceptual):**
    1. Go to **Preferences > My Access Keys** and generate a new Access ID and Key. **Immediately copy and save them somewhere safe, as they are shown only once.**
    2. **Conceptual:** Think about how you might use `curl` or a simple Python script to perform a basic action like listing your collectors using the API. (You don't need to write code, just understand the concept from the API docs.)
  - **Activity 2 (Certification Review):**
    1. Review the Sumo Logic Certifications page.
    2. Identify which certification (e.g., Fundamentals, Search Mastery) aligns best with what you've learned.
    3. Consider taking a practice exam if Sumo Logic offers one on their learning portal for the "Fundamentals" certification.

General Tips for Success:

- **Consistency is Key:** Try to dedicate a consistent block of time each day.
- **Troubleshoot:** When you encounter issues, refer to the Sumo Logic documentation and community forums.
- **Review:** At the end of each day, briefly review what you've learned.
- **Don't Rush:** It's a lot of information. Prioritize understanding over speed.
- **Take Notes:** Keep a separate set of notes for key concepts, SPL commands, and tips.

This structured approach, combined with active hands-on engagement, will give you a robust foundation in Sumo Logic. Good luck!