sumo logic
Academy

Cloud SIEM

Student Lab Guide

Rev 10.29.25.K

©2025 Sumo Logic, All Rights Reserved.

Disclaimer

This course material is Sumo Logic, Inc. confidential information. Sumo Logic, Inc. provides it as-is solely for your use and assessment as an individual partaking in the training and certification program on our Learning Portal and in specified other venues. The course material may not be reproduced, sold, or otherwise processed or transferred in any other way or for any other purpose without prior written permission from Sumo Logic. Sumo Logic owns the copyright and other intellectual property rights in the text, graphics, information, designs, data, and other content on this website (including exam materials and certifications as well as audio files and their scripts) with the exception of our partners', licensors', and other third parties' trademarks and other intellectual property. United States export control laws and regulations apply to this material, and you agree to comply with such laws and regulations.

©2025 Sumo Logic, All Rights Reserved.

sumo logic
Academy

Table of Contents

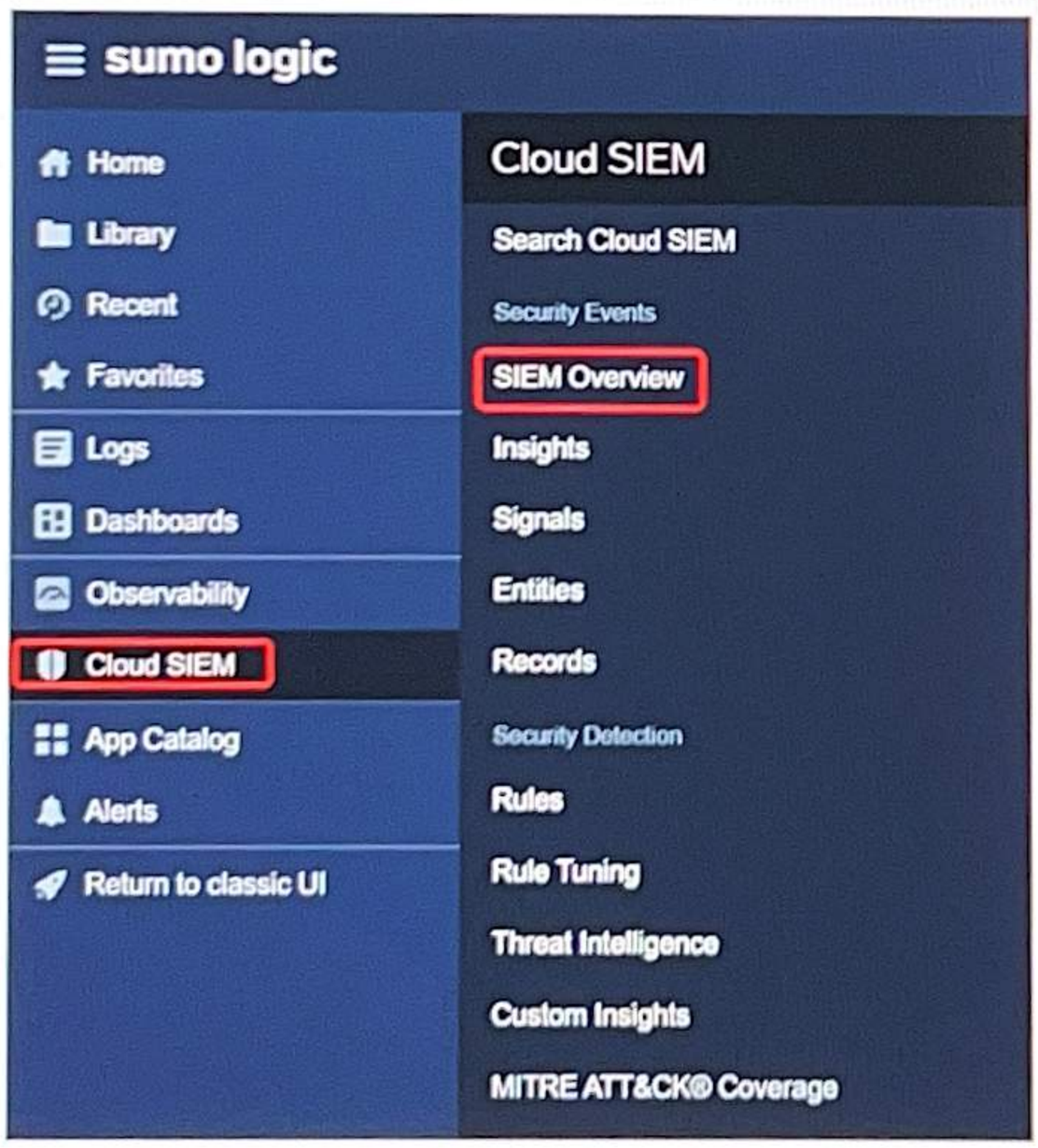
- Disclaimer
- Table of Contents
  - Lab 0: Log in to the training environment
  - Lab 1: Explore the Cloud SIEM UI
  - Lab 2: Investigate an Insight
  - Lab 3: Continue the investigation into Sumo Logic Search
  - Lab 4: Enable data forwarding for an HTTP source
    - Tips and tricks
  - Lab 5: Sending a sample log message to Cloud SIEM
    - Tips and tricks
  - Lab 6: Creating a data parser in Sumo Logic
  - Lab 7: Set up a log mapping
    - Tips and tricks
  - Lab 8: Send another log message to Cloud SIEM
    - Tips and tricks
  - Lab 9a: Create a custom match rule
  - Lab 9b: Write a threshold rule
  - Lab 9c: Write a chain rule
  - Lab 9d: Write an aggregation rule
  - Lab 9e: Write an outlier rule
  - Lab 9f: Write a first seen rule
  - Lab 10: Create a rule tuning expression
  - Lab 11: Create a custom Insight
  - Lab 12: Customize the actions button

©2025 Sumo Logic, All Rights Reserved.

Lab 0: Log in to the training environment

The training lab environment is separate from your other accounts. To access the training lab environment:

1. Open a new browser tab.
2. Go to https://service.sumologic.com.
3. Enter **training+admin###@sumologic.com** in the **Email** field. Replace ### with a three digit number between 000 and 999.
4. Enter the **Password** provided to you by your instructor.
   Note: The password changes monthly.
5. In the left navigation menu, click **Cloud SIEM > SIEM Overview** to go to the Cloud SIEM training environment.



That's it! You'll be redirected to the Cloud SIEM heads-up display (HUD).

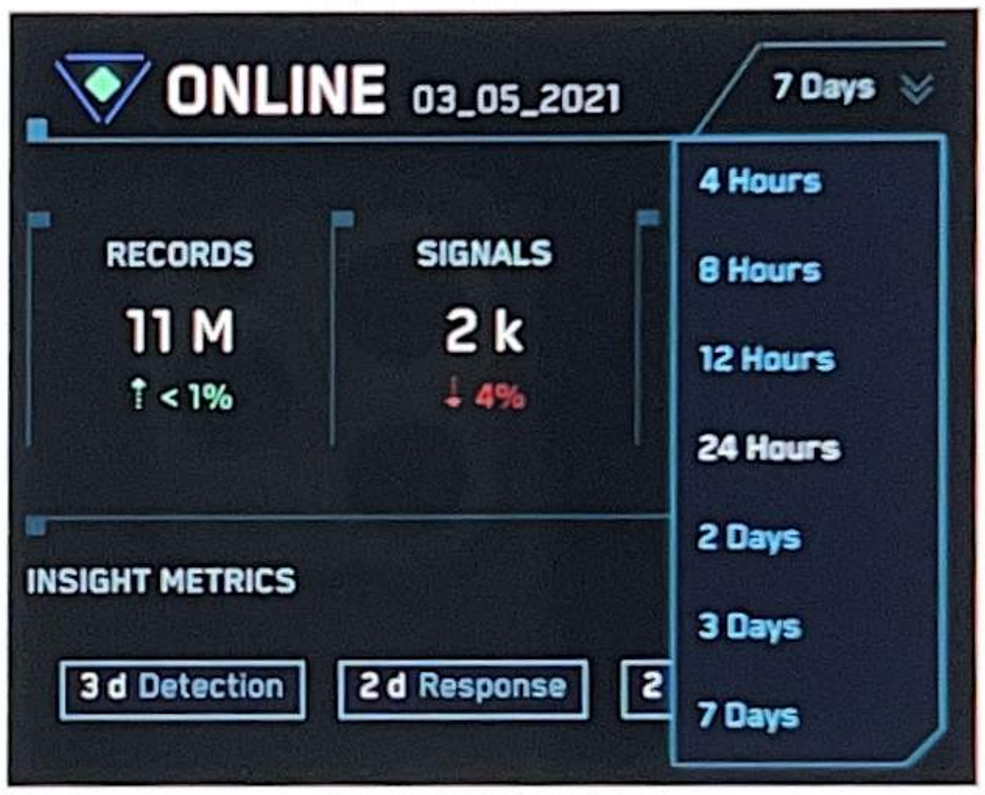
Note: The training environment is a **shared, dynamic environment.** The data is refreshed and cleaned periodically. Other students can see the comments you make, so be careful what information you share. The dynamic updates and activities of other students may affect the data you see. Your experience will vary from one session to the next.

©2025 Sumo Logic, All Rights Reserved.

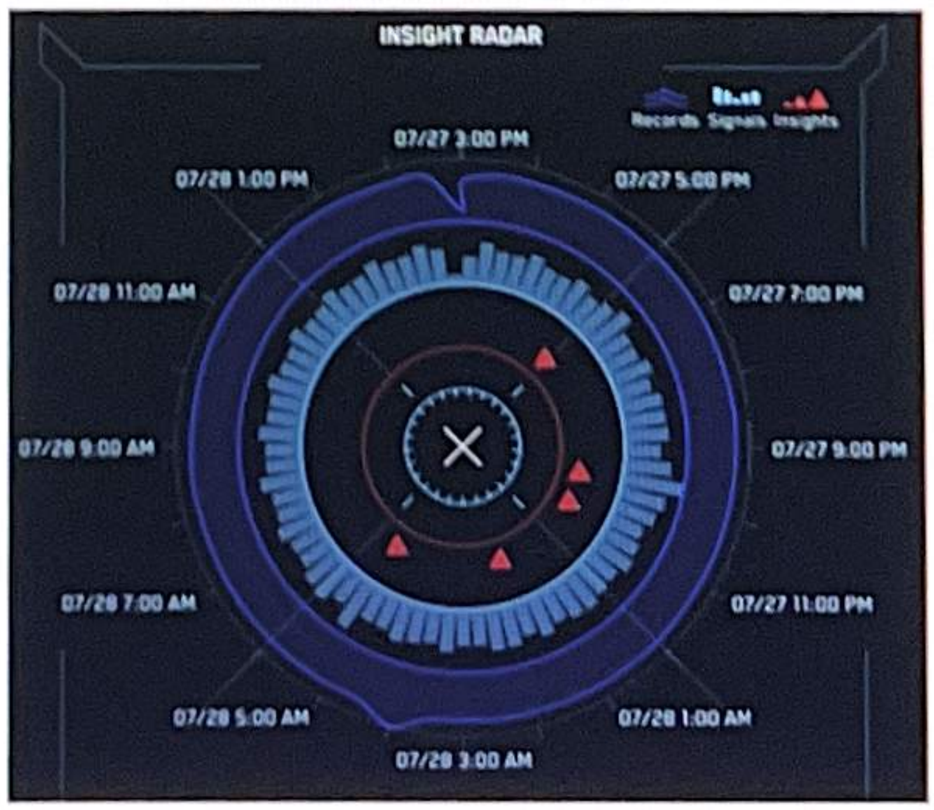
Lab 1: Explore the Cloud SIEM UI

Navigate to the Cloud SIEM HUD. Refer to Lab 0 if you need help.

1. Near the top of the left pane of the Cloud SIEM UI, you'll see summary statistics. In the upper right corner of this pane, a dropdown menu lets you select the timeframe for the summary statistics. Use the summary panel and the dropdown to answer these questions:
   a. How many Records have been ingested in the last 8 Hours?
   b. How many Signals have been created in the last 7 Days?
   c. How many Insights have been created in the last 24 Hours?



2. In the center of the Cloud SIEM HUD is the Insight Radar. Hover over each piece of the Insight Radar to answer these questions:
   a. What time were the most Records ingested in the last 24 hours? When were the fewest records ingested? **Hint**: Hover over the blue line to find out how many Records were ingested at each time increment.
   b. What time were the most Signals created in the last 24 hours? When were the fewest Signals created? **Hint:** Hover over each bar to find out how many Signals were generated at each time increment.



©2025 Sumo Logic, All Rights Reserved.

c. How many Insights have been generated in the last 24 hours? **Hint:** Each triangle represents one or more Insights, so hover over each to find the number of Insights each represents.

3. In the left navigation menu, click **Cloud SIEM**, then **Rules** (under the **Security Detection** header). Remove any filters from the **Filters** bar. Then, use the **Filters** bar to answer these questions:
   a. How many rules have a name that contains "firewall"? **Hint:** enter any keyword into the filter bar to search for that keyword.
   b. How many rules have a severity score greater than 8? **Hint**: enter "severity" then choose "greater than", then enter "8"
   c. How many rules detect the "persistence" tactic? **Hint**: select "Tags" > "contain" > "Tactic" then choose "Persistence"
4. In the left navigation menu, click **Cloud SIEM > Entities**. Remove any filters from the **Filters** bar. Use the **Filters** bar to answer these questions:
   a. How many entities have an activity score of 5 or greater? **Hint:** Use the autocomplete suggestions and dropdown menus to enter **Activity Score greater than 5** in the **Filters** bar.
   b. How many entities have an activity score of 0?
   c. **Discussion:** What does an entity with an activity of zero mean?
5. Click **Cloud SIEM > SIEM Overview** in the left menu to return to the main Cloud SIEM HUD.

Your answer to all these questions may vary. Be sure to share your findings with your classmates. If you have trouble finding any information, ask your instructor to demonstrate.

Tips and tricks

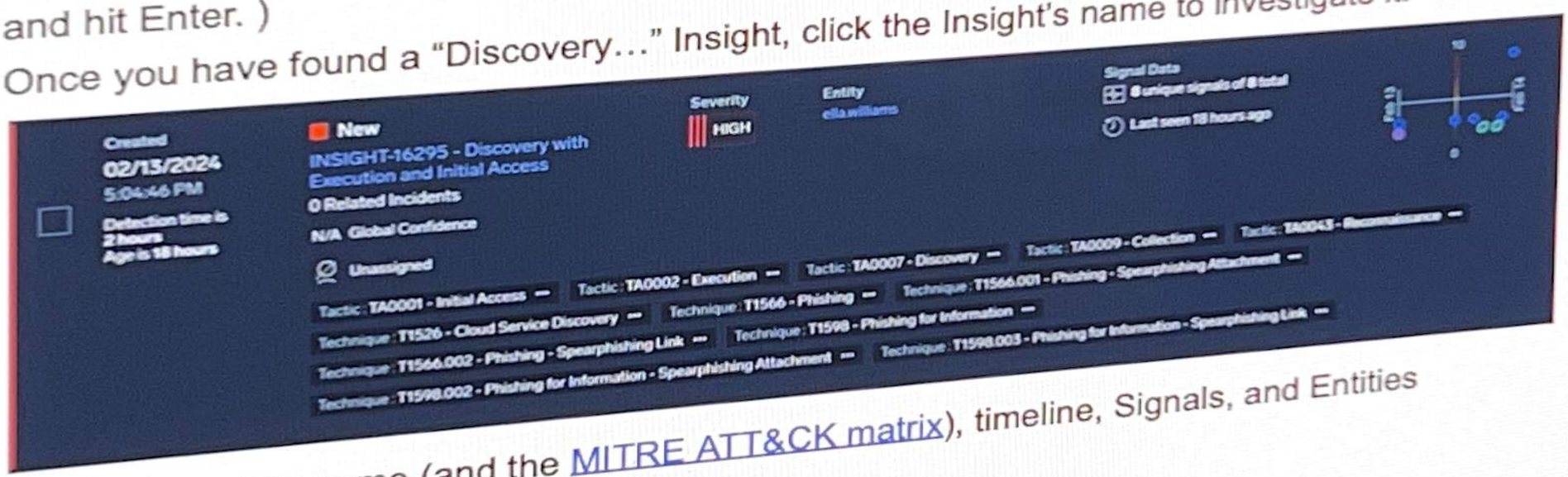
- Filters persist each time you search. This is great if you want to drill down into subsets of data. For this exercise, you'll need to remove all filters before answering each question.

©2025 Sumo Logic, All Rights Reserved.

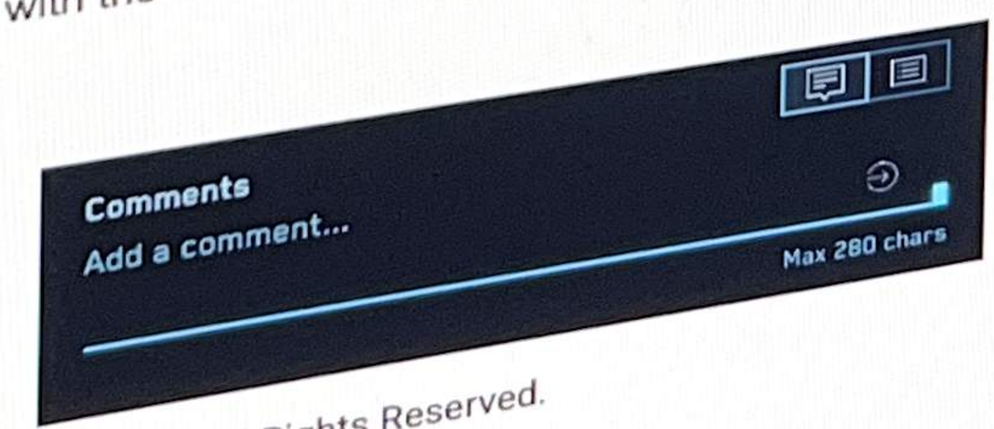
Lab 2: Investigate an Insight

In this lab, you'll be investigating an insight for your organization that was detected through Cloud SIEM. Our goal is to analyze the insight details and complete the narrative of what happened.

1. In the left navigation menu, click **Cloud SIEM > Insights**.
2. Find an Insight named **Discovery with Execution and Initial Access**. (If no insights with this name are visible on the first page, type in "Discovery" into the filter bar on top and hit Enter.)
3. Once you have found a "Discovery…" Insight, click the Insight's name to investigate it.



4. Use the Insight's name (and the MITRE ATT&CK matrix), timeline, Signals, and Entities to answer these questions before moving on:
   a. What events (Signals) were detected and correlated together?
   b. What is the total of all the severity scores of the Signals in this Insight?
   c. What order did the events happen in?
   d. What hypotheses do you have about how and why the event happened?
   e. What other information can you find by exploring this Insight?
5. Scroll to the bottom of the left navigation pane of the Insight. Write a short summary of your answers from Step 4 in the **Comments** section.
   a. Use your unique identifier in your comment (your initials and/or your three digit login ID).
   b. Compare your summary with the one below.



Summary: First, a known phishing link was received in a user's email. A few minutes later, a malicious file was allowed. It seems the user clicked a

©2025 Sumo Logic, All Rights Reserved.

Lab 3: Continue the investigation into Sumo Logic Search

Follow along with your instructor as they demonstrate this investigation.

In the previous lab, we looked at an Insight called **Discovery with Execution and Initial Access**. In this lab, we will use Sumo Logic Search to continue the investigation. Then, we will update the status of your investigation in Cloud SIEM.

1. Return to the **Discovery with Execution and Initial Access** Insight. If you're not there already, refer to lab 2 for help in navigating back to the Insight record.
2. In the left pane, hover over the Entity (will usually be a user name such as "ava.scott" or an IP address). Click the **context actions** (six dots) icon that appears.

3. From the dropdown (under **Actions**), select **Sumo Logic Search**. You may need to scroll to find it. You'll be redirected to Sumo Logic Search. .
4. Make a note of the entity name that's pre-populated in the query builder.

```
1   ava.scott
```

5. Open another log search in Sumo Logic with **Logs > Log Search**.
6. Find the top 10 records by threat type. In the search bar, type or copy:

```
_index=sec_record_*
| where !isEmpty(threat_name) and
user_username="<username>"
| count by threat_name
| topk(10, _count)
```

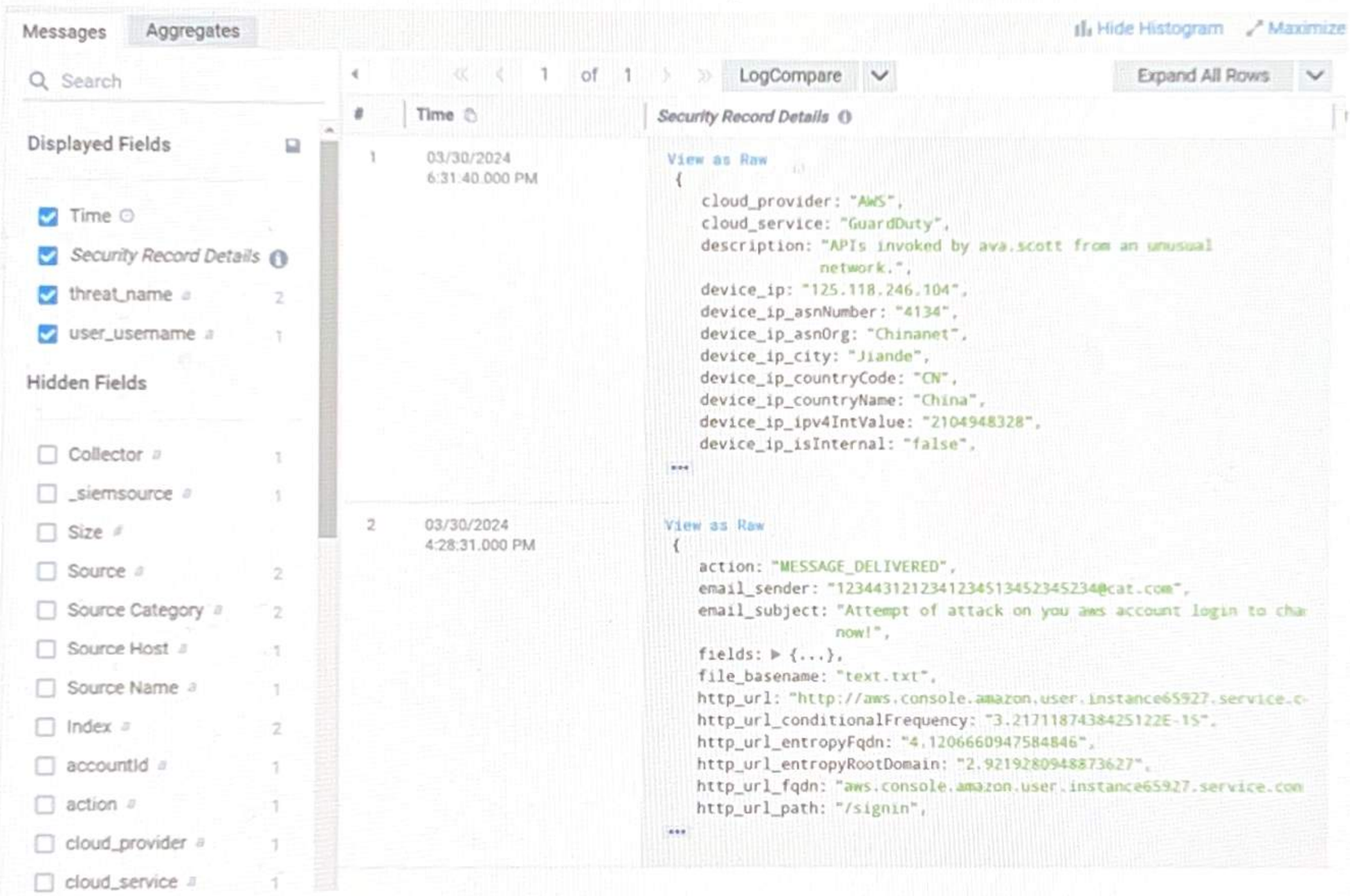
Replace <username> with the user name from Step 4.

-3d

```
1  _index=sec_record_*
2    | where !isEmpty(threat_name) and user_username="ava.scott"
3    | count by threat_name
4    | topk(10, _count)
```

©2025 Sumo Logic, All Rights Reserved.

1. Click **Start** to run the log search.
    a. Make sure your quotes are straight! Copy and pasting the command sometimes changes the formatting of these quote marks into curly quotes.
    b. You may need to increase the time of the search to the **Last 24 hours** or **Last 3 Days** to see results. The default is the **Last 15 minutes**.
    c. Make sure you're viewing the **Messages** tab when the results load.



The `_index=sec_record_*` searches all records ingested into Cloud SIEM. This particular query excludes those with nothing in the `threat_name` value. Additionally, it sorts it by threat name, and shows the most frequent threats. This will help you identify everything this user was doing around this timeframe, to see if anything not caught by the Cloud SIEM rules sticks out.

If you have trouble finding any information, ask your instructor to demonstrate.

Finish the investigation

1. When you're done exploring the raw logs, return to the Cloud SIEM tab.
2. If you think there's **still more work** to do, use the **Status** dropdown to record your progress. Here, you can set the

©2025 Sumo Logic, All Rights Reserved.

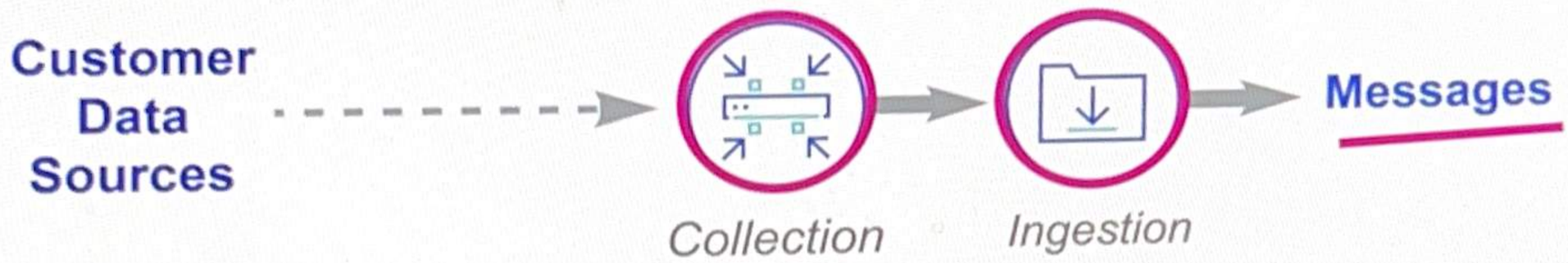
Insight as **In Progress**, escalate it by assigning it to the **SpecOps** or **Tier 3** analyst teams, or set the Insight to **Closed.**

3. If you've **finished your investigation**, use the **Close Insight** button or use the **Status** dropdown to set the status to **Closed**. Then, select whether the Insight has been resolved, is a false positive, if no action is required, or if it's a duplicate.

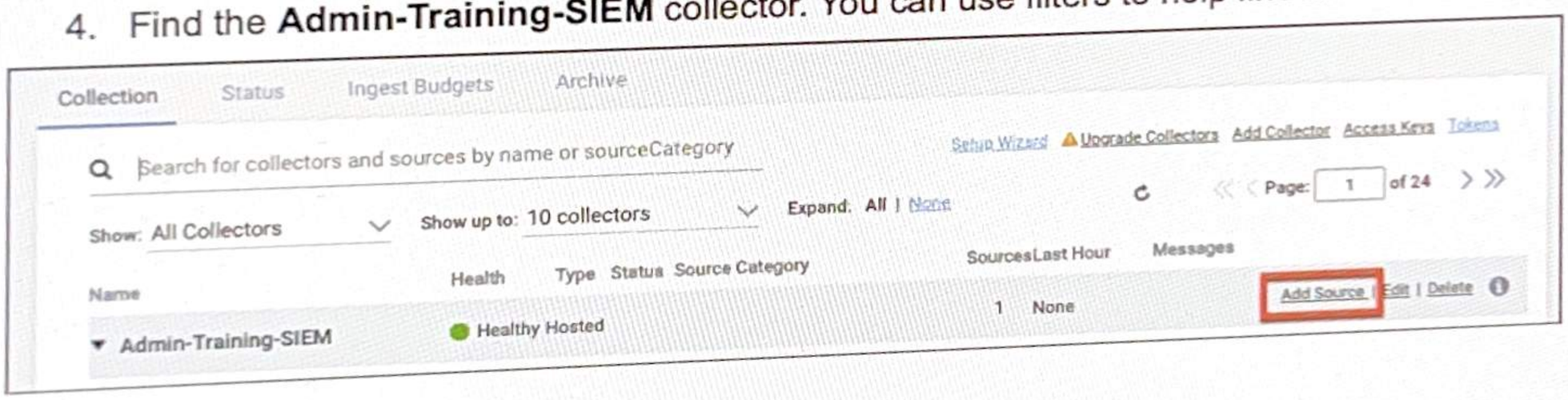
©2025 Sumo Logic, All Rights Reserved.

Lab 4: Enable data forwarding for an HTTP source

In this lab, we'll create a simple HTTP source in Sumo Logic, using a pre-configured collector. When we configure the new source, we'll enable data forwarding to Cloud SIEM. Once the new source is configured with data forwarding, we'll be able to send data to it and observe the data flow.

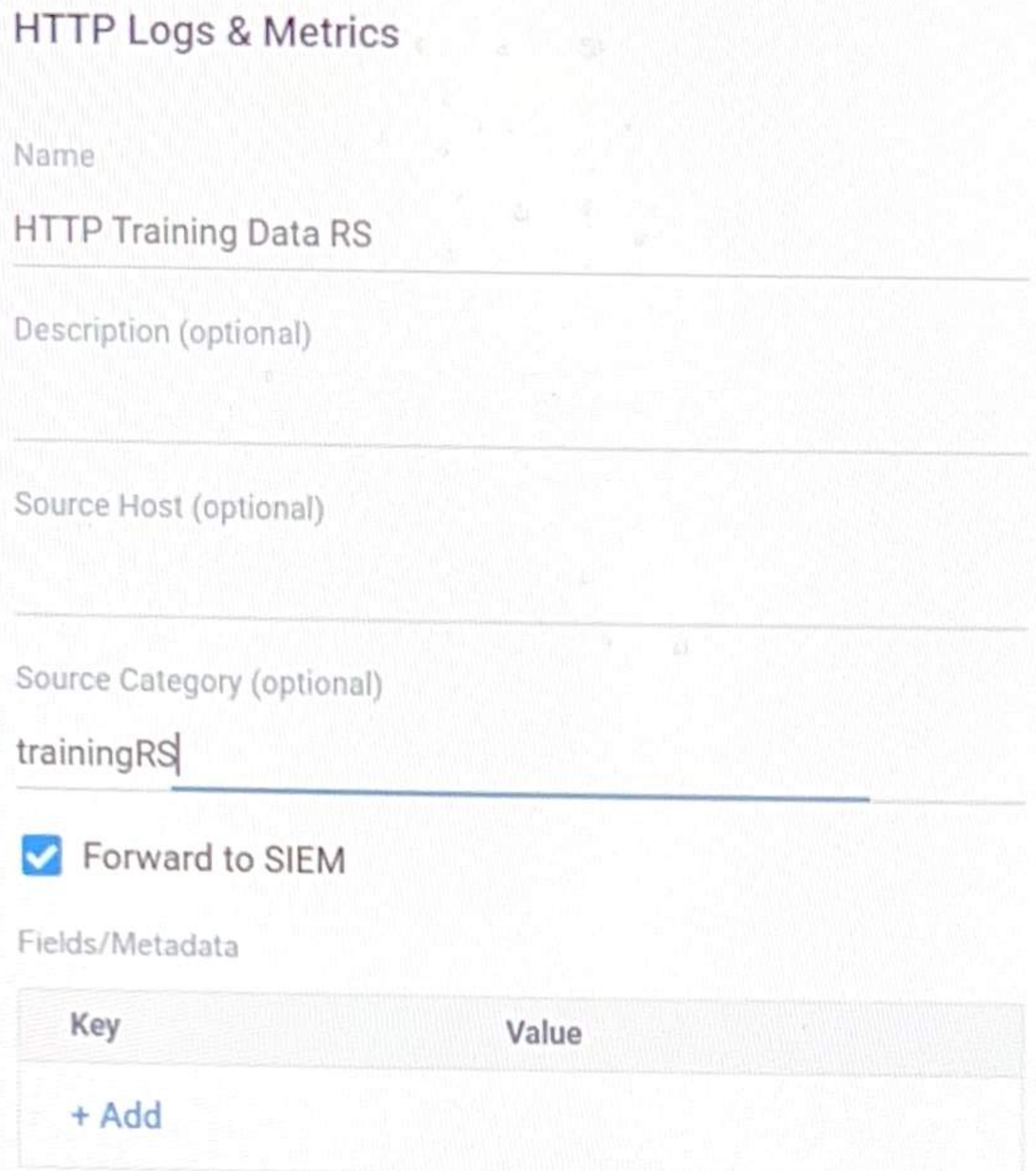


1. Navigate to the Sumo Logic UI, if you're not already there.
   a. Refer to Lab 0 if you need help logging in.
2. In the left nav menu of the Sumo Logic UI, click **Data Management > Collection**.
3. Make sure you're in the **Collection** tab.
4. Find the **Admin-Training-SIEM** collector. You can use filters to help find it.



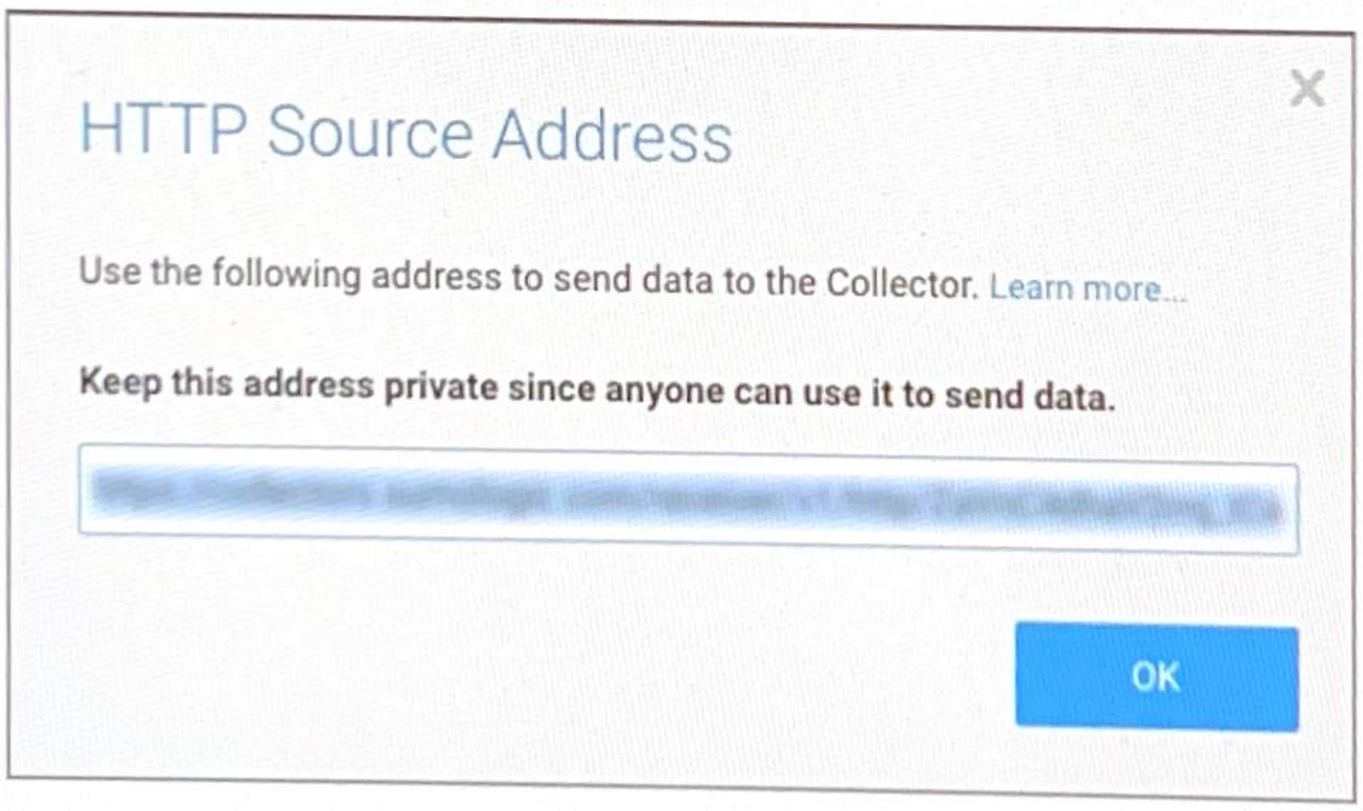
5. Click **Add Source**.
6. Click **HTTP Logs & Metrics** (under the **Generic** category).
7. Enter a **Name**, "HTTP Training Data XXX" with XXX replaced with your initials.
8. Enter a **Source Category**, "trainingXXX" using your initials in place of the XXX.
9. Click the **Forward to SIEM** checkbox.

©2025 Sumo Logic, All Rights Reserved.



10. Leave other fields as their defaults, then click **Save**.

11. A popup will appear with a URL. Copy the URL and keep it somewhere safe, like a Notes or TextEdit file. We'll use it in the next lab.



©2025 Sumo Logic, All Rights Reserved.

Tips and tricks

- Read the best practices for source category design and a detailed explanation of data forwarding.
- If you need to find the HTTP source URL address again, click the Show URL button next to your source.

©2025 Sumo Logic, All Rights Reserved.

Lab 5: Sending a sample log message to Cloud SIEM

In this lab, we'll send a simple JSON log message to the HTTP source we created in the previous lab. Then, we'll look for that log message in Cloud SIEM. This will verify that we configured our source correctly in Lab 4, and demonstrate how quickly Cloud SIEM can ingest data.

1. Open a CLI window, such as Terminal or PowerShell.
2. Type or copy this command:

   (Windows)

   ```
   Invoke-WebRequest -Uri <http source url> -Method POST
   -ContentType "application/json" -Body '{"ip": "127.0.0.1",
   "threatName": "trainingXXX"}'
   ```

   (macOS)

   ```
   curl -d '{"ip": "127.0.0.1", "threatName": "trainingXXX"}' -H
   'Content-Type: application/json' <http source url>
   ```

   Replace the XXX in "trainingXXX" with your own initials or another unique identifier.
   Replace the **`<http source url>`** with the URL you copied in the previous lab.

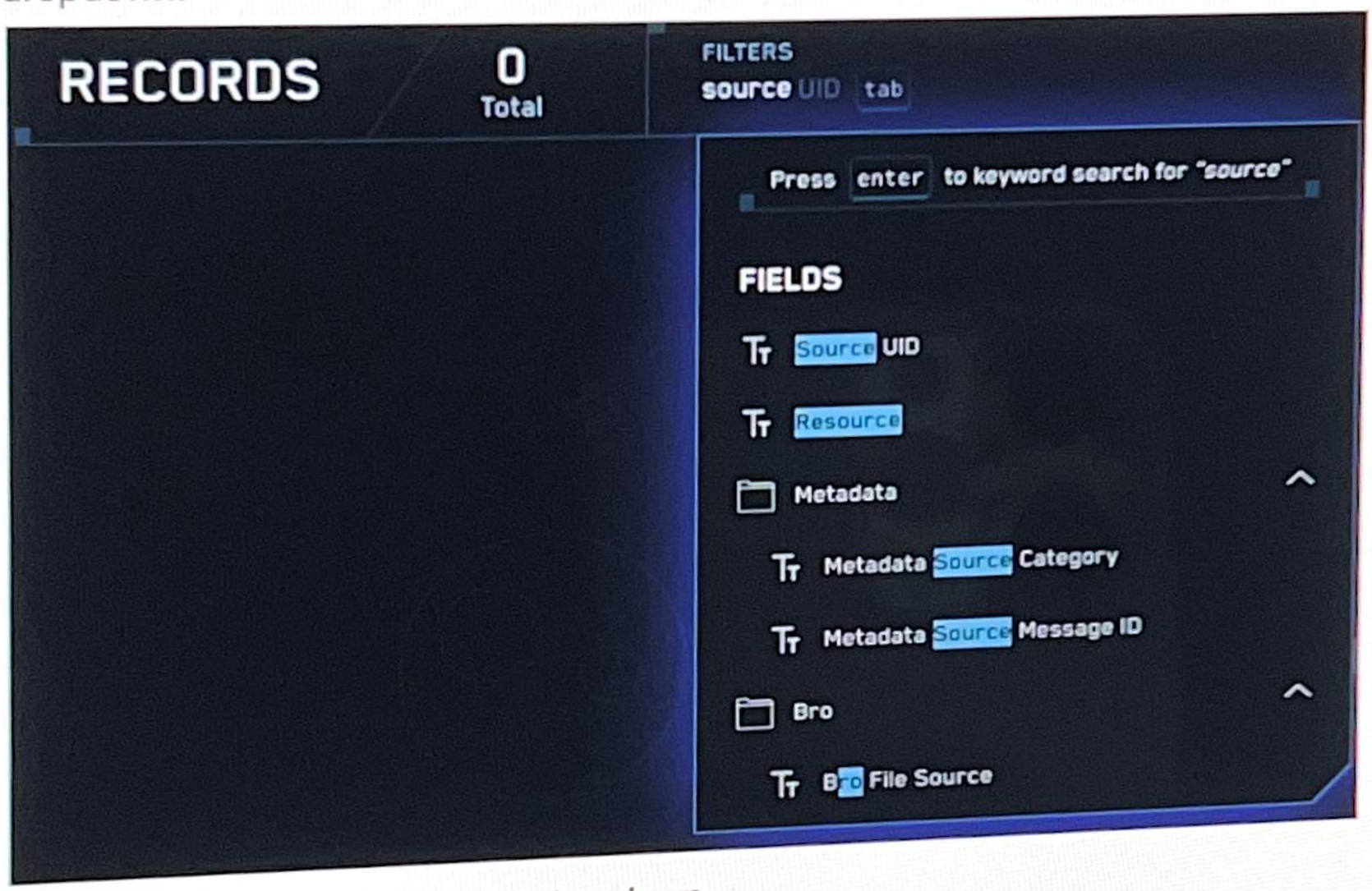
```
[redacted]-mac ~ % curl -d '{"ip": "127.0.0.1", "threat_name": "RS"}'
-H 'Content-Type: application/json' https://collectors.sumologic.com/[redacted]
[redacted]-mac ~ %
```

This simple JSON log message, **`{"ip": "127.0.0.1", "threatName": "trainingRS"}`**, will be collected and ingested by Sumo Logic as soon as you hit Enter. If data forwarding was enabled properly in the previous lab, it's also forwarded to Cloud SIEM where it's parsed, mapped, and enriched. This process can take anywhere from a few seconds to up to 5 minutes. Now's a great time to get up, stretch, and grab a beverage.

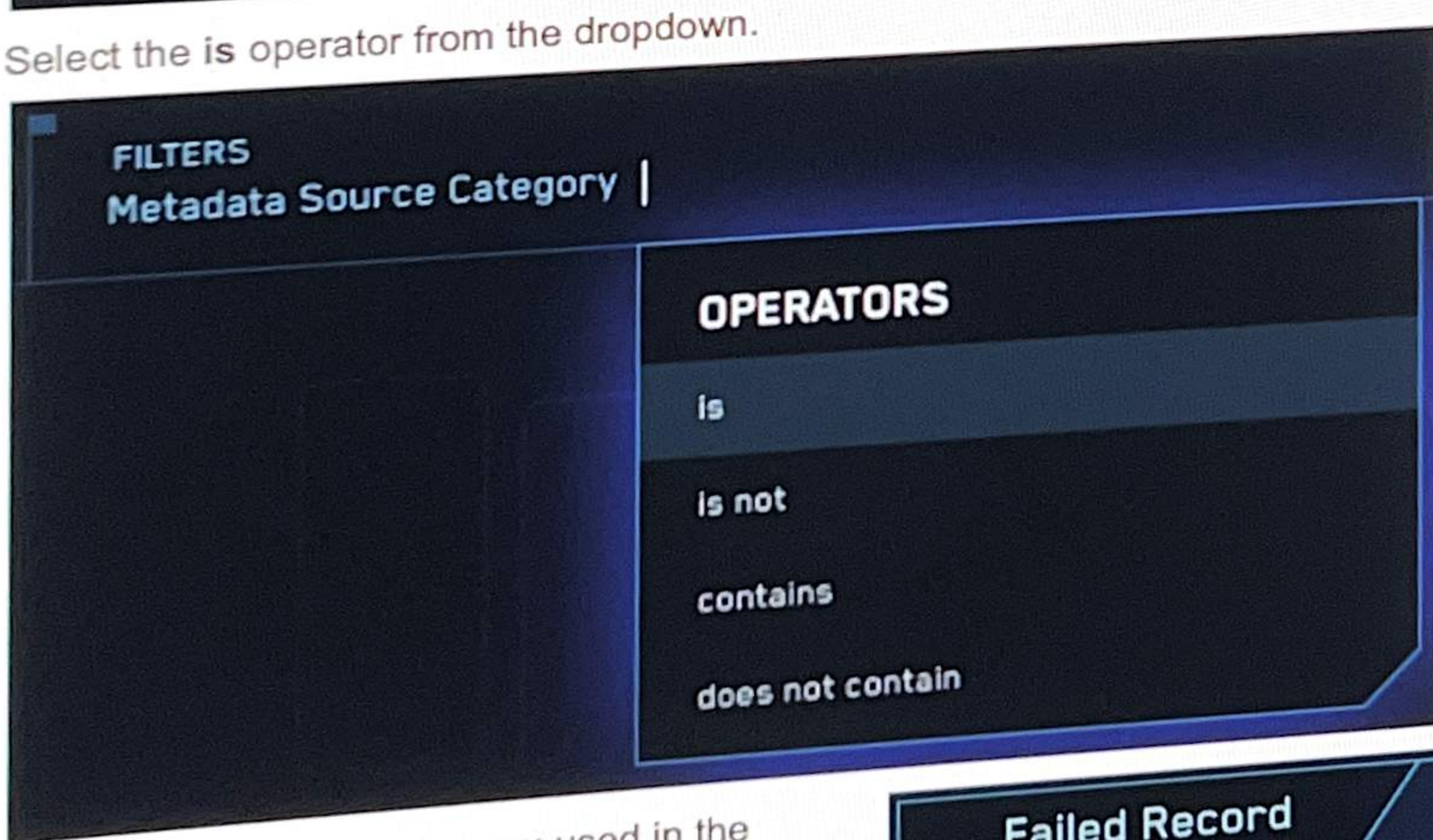
©2025 Sumo Logic, All Rights Reserved.

When you're ready, we'll find your log message as a record in Cloud SIEM.

3. In the left navigation menu, click **Cloud SIEM > Records**.
4. In the **Filters** bar, type "source" to search for **Metadata Source Category** from the dropdown.



5. Select the **is** operator from the dropdown.



6. Type the source category you used in the previous lab.

©2025 Sumo Logic, All Righ

7. You should see a failed record.

This record failed because the custom JSON log message does not have a parser or log mapping associated with it. Although the log message was forwarded from Sumo Logic to Cloud SIEM, it did not successfully complete the parse, map, and enrich steps of the pipeline. We'll fix this in the next lab activities.

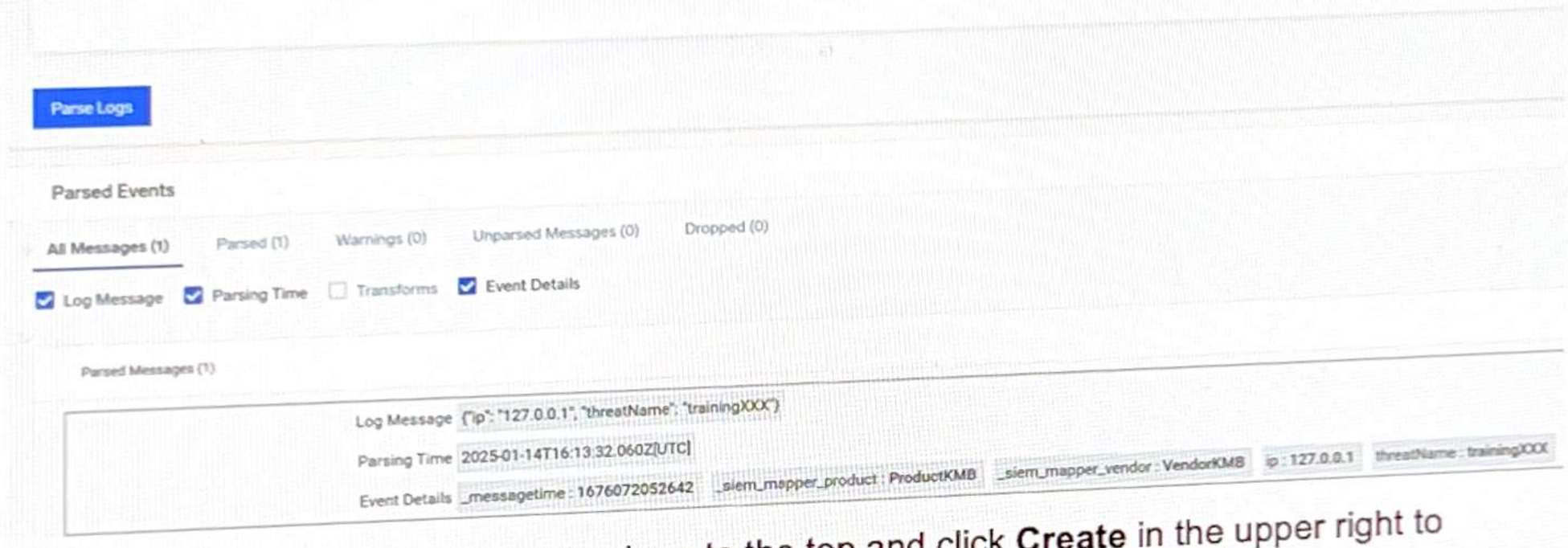
Tips and tricks

- If you get an error after running the console command in Step 2, make sure your quotes are straight! Copy and pasting the command sometimes changes the formatting of these quote marks into curly quotes.
- If you don't see any records after Step 7, try:
  - increasing the **Timestamp** range to the **Last 60 minutes** or the **Last 3 hours**
  - making sure the metadata source category you searched in the **Filters** bar matches the one you created in the previous lab.
  - searching for the log in Sumo Logic with this query: `_index=sec_record_* metadata_sourceCategory=trainingRS` Replace trainingRS with the source category you created.
- If you still don't see your custom JSON record after these troubleshooting steps, try sending another log message from your terminal window (Steps 1 and 2 of this lab). Make sure the command completes without any errors.

©2025 Sumo Logic, All Rights Reserved.

sumo logic Academy

SIEM ingestion process. This test method can also be used to troubleshoot when fields are not showing up in Cloud SIEM and administrators can check whether the fields are being parsed correctly from the original log messages.



13. If all the details are correct, scroll back up to the top and click **Create** in the upper right to finalize your parser.
14. The final step is to tell our collector source to exclusively use our new parser when data is sent to it. Back on the main Parsers list, find your parser and click the 'triple-dot' icon on the far right of the row. Select **Copy Path**.
15. Navigate to the Collection page again (**Data Management > Collection**).
16. Find your custom source "HTTP Training Data XXX" under the "Admin-Training-SIEM" collector you created in the earlier lab and click the **Edit** link on the right side.
17. On the source details view, find the **Fields/Metadata** section and click **+Add**.

©2025 Sumo Logic, All Rights Reserved.

18. In the **Key** field, enter "_parser", and for the **Value** field, paste in the path from your parser.

Source Category (optional)

trainingKMB

☑ Forward to SIEM

Fields/Metadata

Key	Value
⚠ _parser	/Parsers/Training Parser
+ Add	

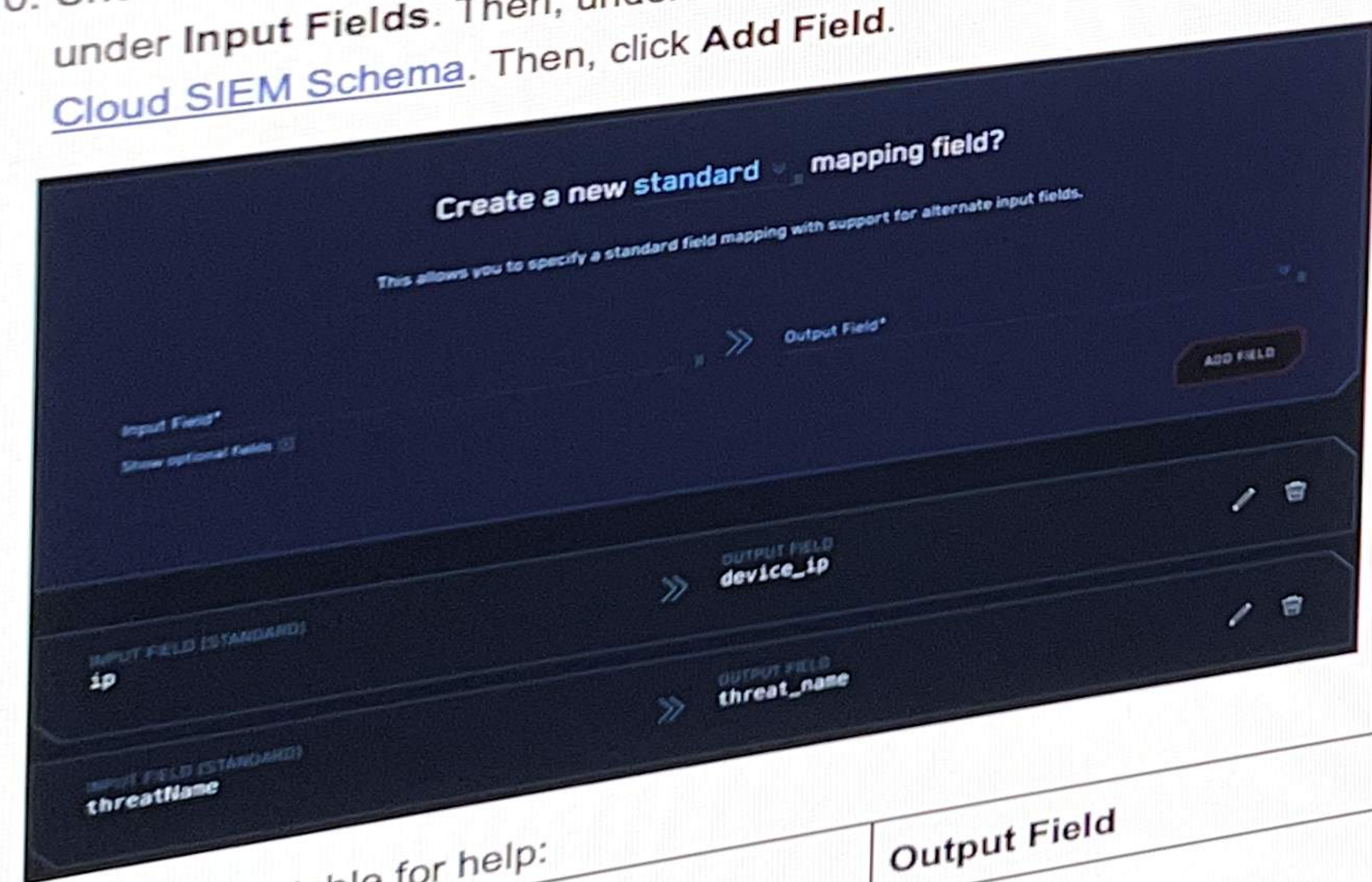
19. Click **Save** to save your source configuration.

©2025 Sumo Logic, All Rights Reserved.

Lab 7: Set up a log mapping

In this lab, we'll create a log mapping to handle the custom log messages we are sending to our collector.

1. In the left navigation menu, click **Cloud SIEM > Log Mappings** (under **Cloud SIEM Integrations**).
2. Click **Create**.
3. Click **Structured Mapping**. In Cloud SIEM, JSON data is considered structured data.
4. Give your log mapping a **Name**, "Log Mapping XXX" with XXX replaced by your initials.
5. Under **If Input Matches**, use the **Vendor** and **Product** you created in your parser in the previous lab (VendorXXX / ProductXXX)
6. Select **JSON** as the format.
7. Type `.*` for the regex. This will match all incoming logs.
8. Leave the **Record of type** field blank for now.
9. Under **Then Create Record**, select with **vendor matching input vendor** and **product matching input product**.
10. Under **Fields**, enter the fields from the JSON log message we sent in the previous lab under **Input Fields**. Then, under **Output Fields**, map them to their equivalents in the Cloud SIEM Schema. Then, click **Add Field**.



Refer to this table for help:

Input Field	Output Field
ip	device_ip

©2025 Sumo Logic, All Rights Reserved.

threatName	threat_name

Typically, JSON logs have more than just two fields. In this lab, we're using the simplified example log we sent in the earlier lab, so we only need to add two new fields.

11. Scroll back up to **Then Create Record**.
12. Select **Record of type Authentication**. Selecting the record type now ensures you do not limit the fields you could select in Step 10.
13. Click **Submit**.

Tips and tricks

- Read the Cloud SIEM Schema for a full list of the fields you can map to.
- Hover over the yellow triangle next to the **Submit** button to see a list of errors and warnings that need to be resolved before you can submit.

©2025 Sumo Logic, All Rights Reserved.

Lab 8: Send another log message to Cloud SIEM

Your new parser and log mapping settings won't apply to log messages that were already ingested, but only to new messages. So, to test our new configuration, we'll resend another log message to our HTTP source just like we did in the earlier lab. Then, we'll look for that new log message in Cloud SIEM. This time, the combination of parser and log mapping we created will apply to the new record.

1. Switch back to your CLI Terminal/PowerShell window (or open a new one).
2. If you are using your original window, since you already sent a console command once, you can usually press the **Up Arrow** key and **Enter** to send the command again in most CLI programs.
   a. If that works, skip to Step 4. Otherwise, complete Step 3.
3. Type or copy this command:

   (Windows)

   ```
   Invoke-WebRequest -Uri <http source url> -Method POST
   -ContentType "application/json" -Body '{"ip": "127.0.0.1",
   "threatName": "trainingXXX"}'
   ```

   (macOS)

   ```
   curl -d '{"ip": "127.0.0.1", "threatName": "<attacker name>"}'
   -H 'Content-Type: application/json' <http source url>
   ```

   Replace the XXX in "trainingXXX" with your own initials or another unique identifier.
   Replace the **`<http source url>`** with the URL you copied in Lab 2.

```
[redacted]-mac ~ % curl -d '{"ip": "127.0.0.1", "threat_name": "RS"}'
-H 'Content-Type: application/json' https://collectors.sumologic.com/[redacted]
[redacted]-mac ~ %
```

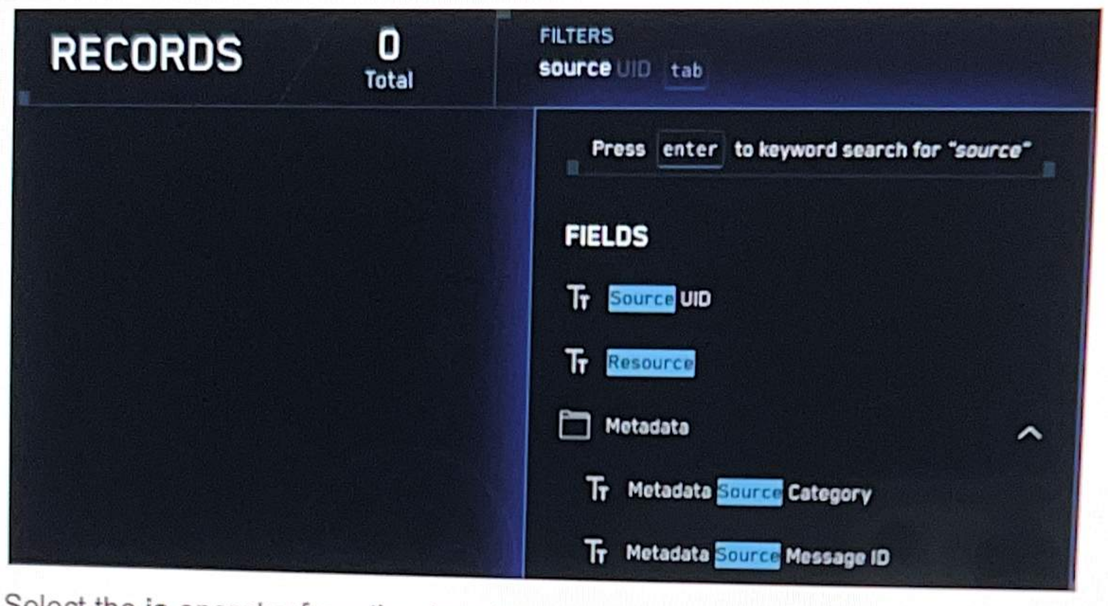
As before, this process can take anywhere from a few seconds to up to 5 minutes. Get up, stretch, or grab another beverage.

When you're ready, we'll find your log message as a record in Cloud SIEM.

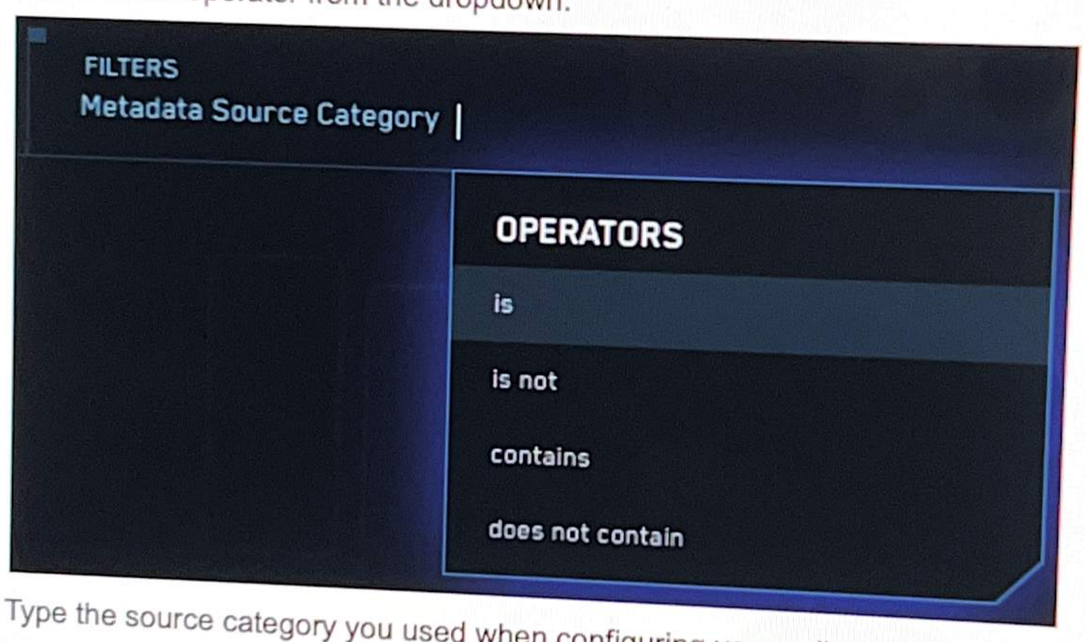
4. In the left navigation menu, click **Cloud SIEM > Records**.

©2025 Sumo Logic, All Rights Reserved.

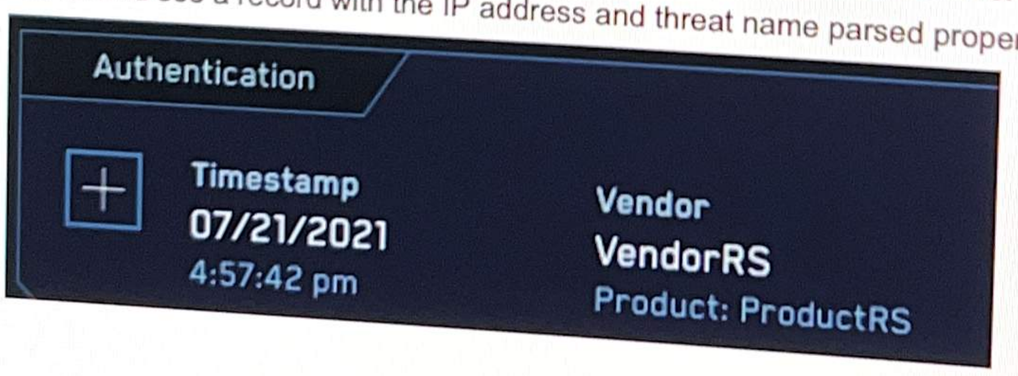
5. In the **Filters** bar, type "source" to search for **Metadata Source Category** from the dropdown.



6. Select the **is** operator from the dropdown.



7. Type the source category you used when configuring your collector source.
8. You should see a record with the IP address and threat name parsed properly.



©2025 Sumo Logic, All Rights Reserved.

After we configured our parser and log mapping in the previous labs, the new log messages forwarded to Cloud SIEM here have now successfully completed the parse, map, and enrich steps to become a record.

Tips and tricks

- If you get an error after running the CURL command in Step 2, make sure your quotes are straight! Copy and pasting the command sometimes changes the formatting of these quote marks into curly quotes.
- If you don't see any records after Step 7, try:
  - increasing the **Timestamp** range to the **Last 60 minutes** or the **Last 3 hours**
  - making sure the metadata source category you searched in the **Filters** bar matches the one you created in the previous lab.
  - searching for the log in Sumo Logic with this query: `_index=sec_record_* metadata_sourceCategory=trainingRS` Replace trainingRS with the source category you created.
- If you still don't see your custom JSON record after these troubleshooting steps, try sending another log message from your terminal window (Steps 1 and 2 of this lab). Make sure the command completes without any errors.
- If your new record failed also (you see two failed records), either the new parser or log mapping wasn't configured correctly. Review those lab steps and try again.

©2025 Sumo Logic, All Rights Reserved.

Lab 9a: Create a custom match rule

A **match rule** is the simplest rule type in Cloud SIEM. Match rules contain an expression which attempts to match the expression details against record fields, resolving to a TRUE or FALSE value.

In this lab, let's create a match rule that checks for Windows 4723 events (marking when a user password has been changed).

1. Click **Cloud SIEM > Rules** in the left navigation menu (under the **Security Detection** header).
2. Click **Create** in the upper right.
3. Select **Match** rule.
4. **Name** your rule "Training Match Rule XXX" with your initials in place of the XXX.
5. Use the following expression (checking for 4723 events for changing user password):

```
objectType = 'Authentication'
AND metadata_vendor = 'Microsoft'
AND metadata_product = 'Windows'
AND metadata_deviceEventId = 'Security-4723'
```

6. Configure the **signal** that will be created once the rule is triggered. On the right side, set "user_username" as the Entity.
7. Set "Password Change" as the name.
8. Set the summary to be "User [User Username] changed their password". (Use the '+' button to add a variable token marked with [ ].)
9. Set the description field to be "Test Rule" or a description of your choice.
10. Set the severity to "constant" and the value to 5.
11. Select "Credential Access" as the tag.
12. Select the **Save this rule as a prototype** checkbox.
    a. **Best practice:** Whenever you create a new rule in Cloud SIEM, save it as a prototype so you can monitor its behavior before pushing it to your system live.
13. Click **Submit** to save your rule.
    a. **Tip:** Check for an orange triangle icon next to the submit button before you submit. This will notify you of any errors or warnings (mouse over it to see the specific errors).
14. Verify your rule exists by going to **Cloud SIEM > Rules** (or through the "Rules" link in the upper left). You should see it there.

©2025 Sumo Logic, All Rights Reserved.