Lab Report — Using Basic Search in Splunk

Name: Dhruvish
Date: October 19, 2025
Platform: Splunk Cloud Trial

Objective

The purpose of this lab was to strengthen foundational **Search Processing Language (SPL)** skills within Splunk, focusing on keyword queries, Boolean logic, field/value filters, wildcards, time controls, and simple result shaping techniques like fields, table, dedup, and sort.

These are core competencies for log analysis, security monitoring, and SIEM (Security Information and Event Management) operations.

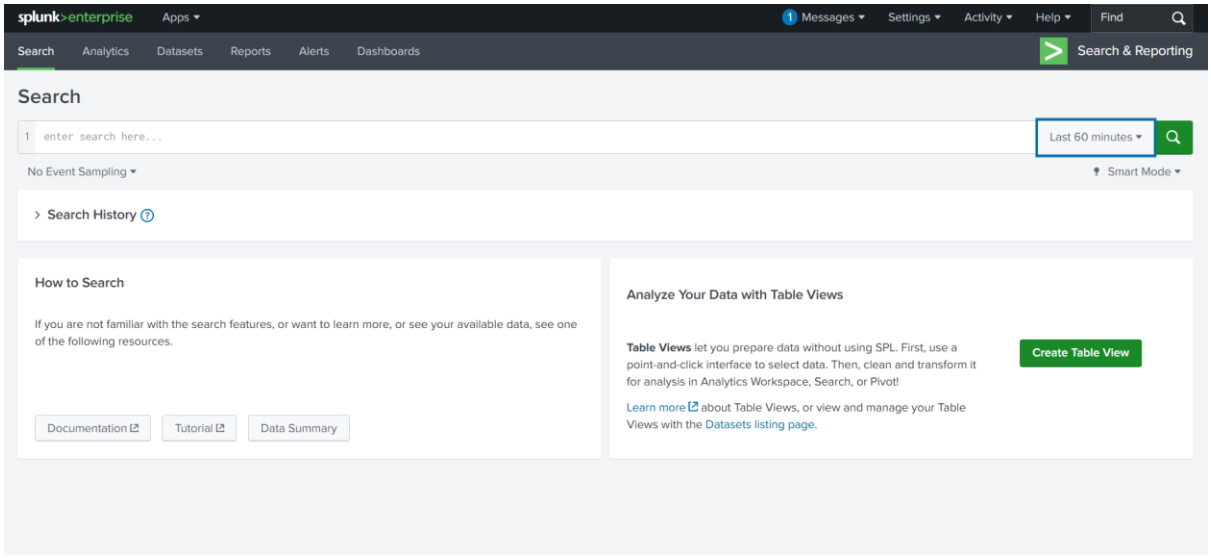
Tools Used

- **Splunk Cloud Trial** (or local Splunk Free installation)
- **Web Browser**

Procedure and Results

Step 1: Open Search & Set Time

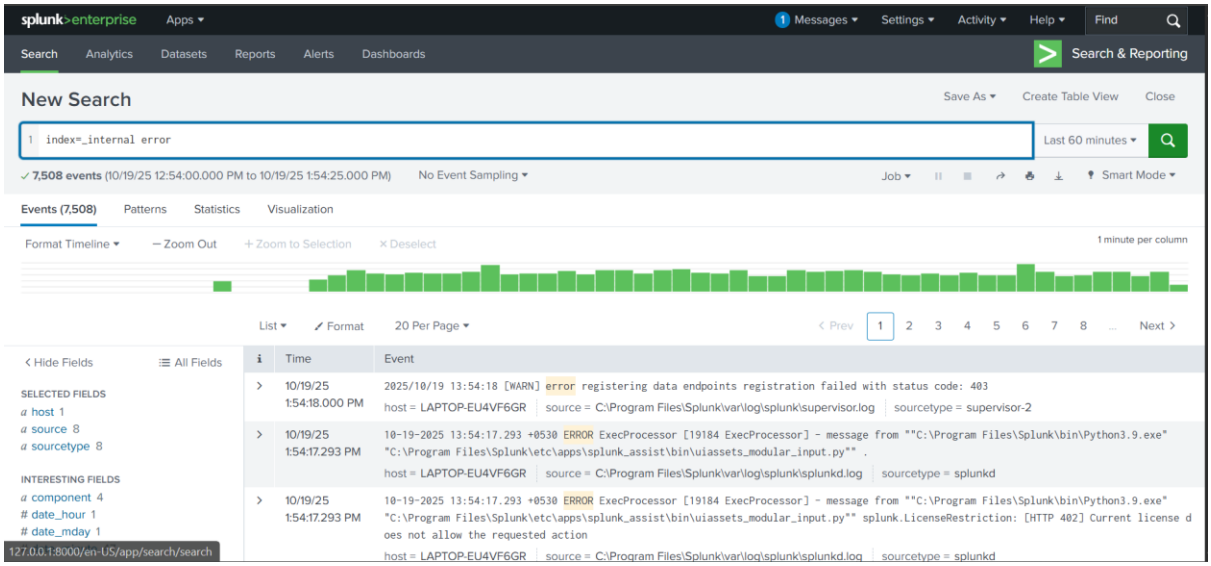
- Logged into **Splunk Cloud Trial**.
- Navigated to **Apps ▸ Search & Reporting**.
- Time range set to **Last 60 minutes**.
- Ensured **Search Mode = Smart**.



Step 2: Keyword & Phrase Search

- **Command:**

  index=_internal error



Returned events containing the keyword “error.”

- **Phrase Search:**

  index=_internal "rest handler"

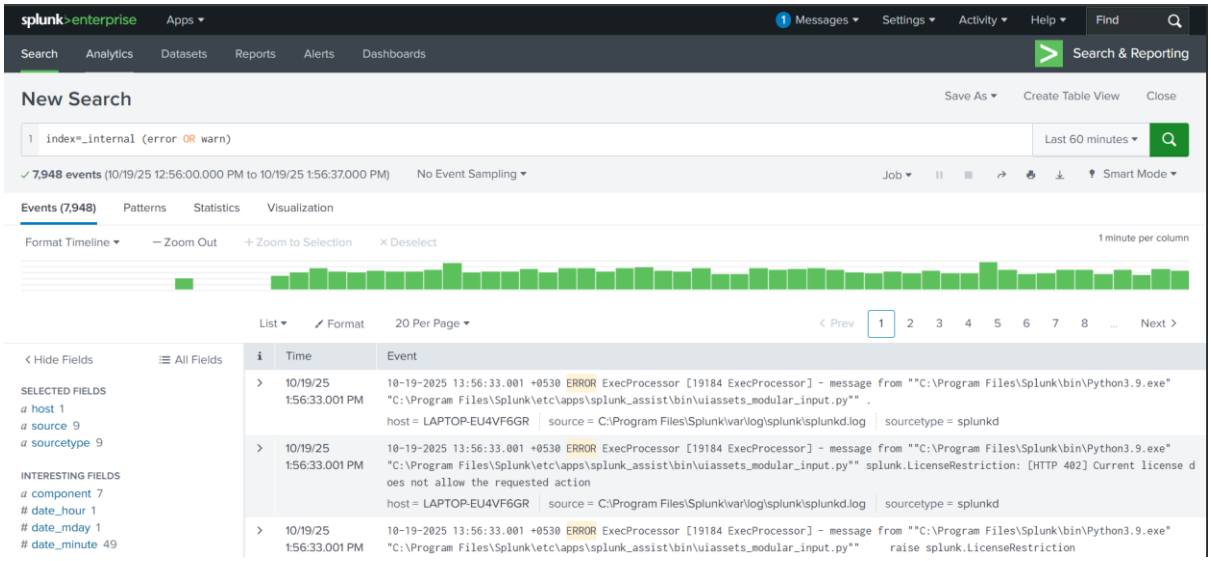
Used quotes for exact phrase matching. Confirmed that searches are **case-insensitive** by default.

Step 3: Boolean Logic

Practiced combining logical operators to refine searches.

- Errors or warnings:

  index=_internal (error OR warn)



- Errors but not UI-related:

  index=_internal error NOT ui

- Grouped logic example:

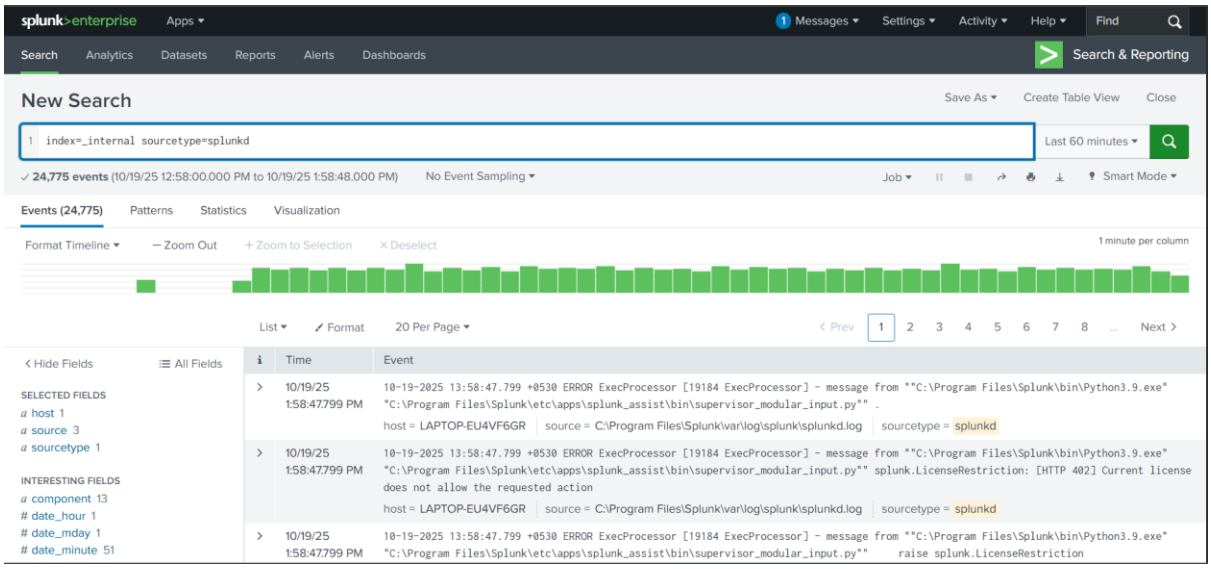
  index=_internal (error OR fail) (http OR tcp)

Step 4: Field/Value Filters

Used field filters for more precise searches.

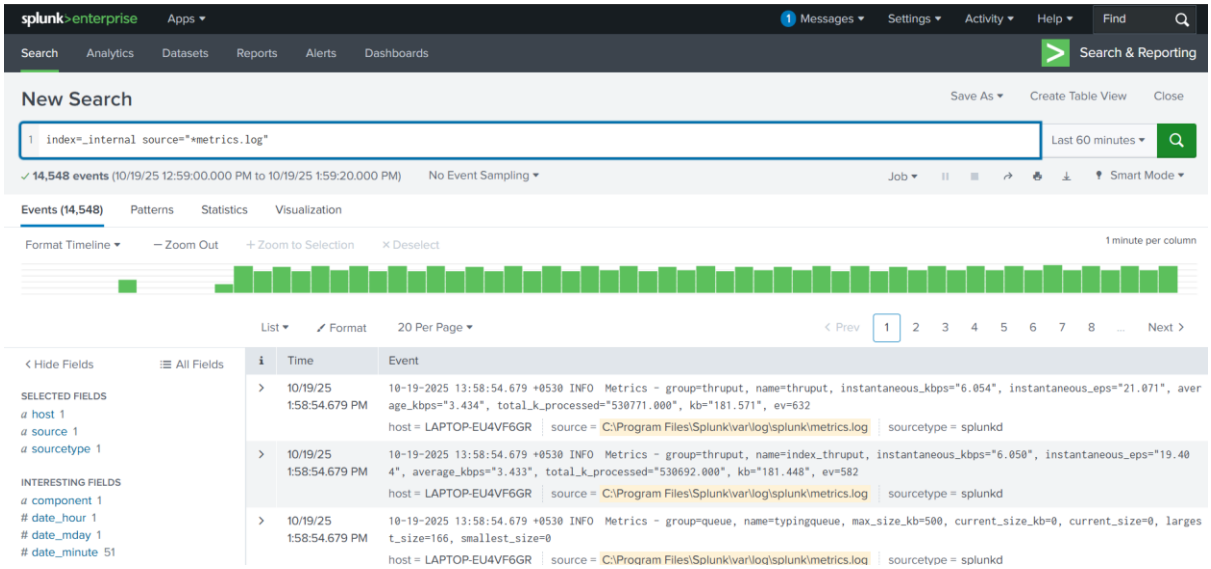
- By sourcetype:

  index=_internal sourcetype=splunkd



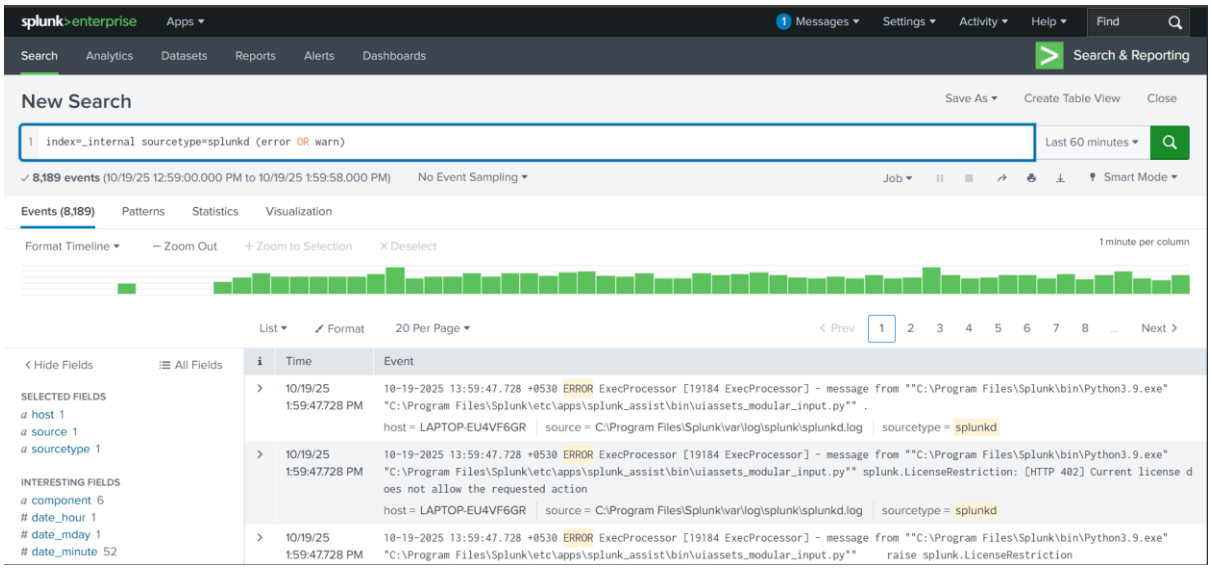
- By source path (wildcard):

  index=_internal source="*metrics.log"



- Combined with Boolean logic:

  index=_internal sourcetype=splunkd (error OR warn)



Step 5: Wildcards & Quoting

Demonstrated wildcard and quoting techniques.

- Wildcard example:

  source="*scheduler.log"

- Quoted value example:

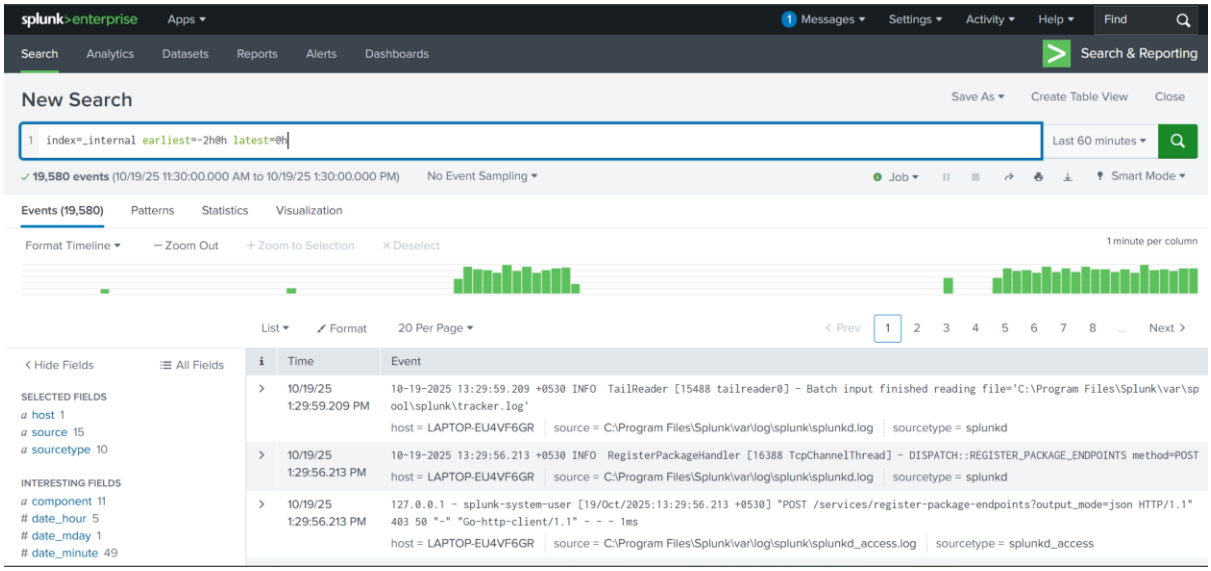
  sourcetype="splunkd_ui_access"

Step 6: Time Control in SPL

Controlled search time windows directly in SPL.

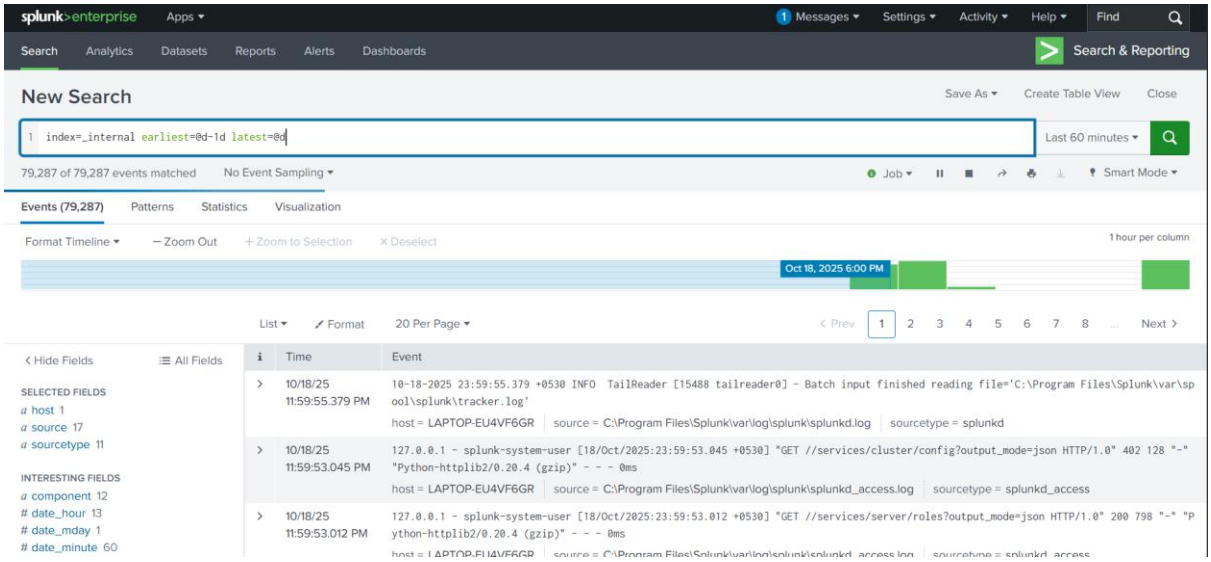
- **Last 2 hours (rounded):**

  index=_internal earliest=-2h@h latest=@h



- **Yesterday only:**

  index=_internal earliest=@d-1d latest=@d



Step 7: Shape the Results

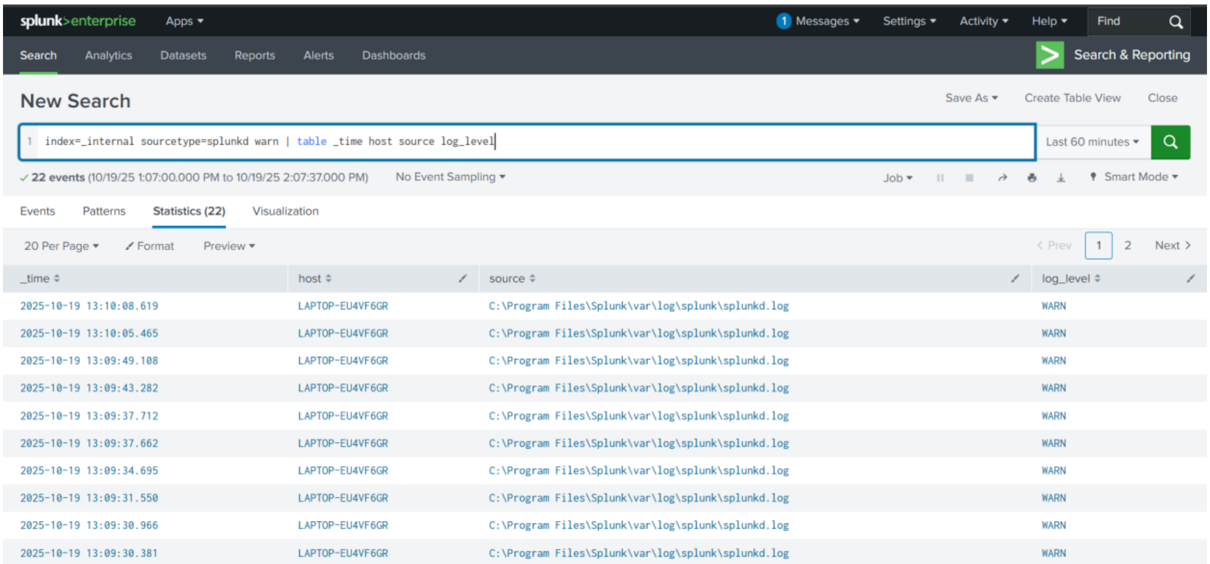
Used result-shaping commands to make data easier to read.

- Select specific fields:

  index=_internal sourcetype=splunkd error | fields _time host source sourcetype

- Create a table view:

  index=_internal sourcetype=splunkd warn | table _time host source log_level



- Display unique hosts only:

  index=_internal sourcetype=splunkd | dedup host | table _time host source

- Sort by newest first:

  index=_internal error | sort - _time

Step 8: Save a Reusable Search (Report)

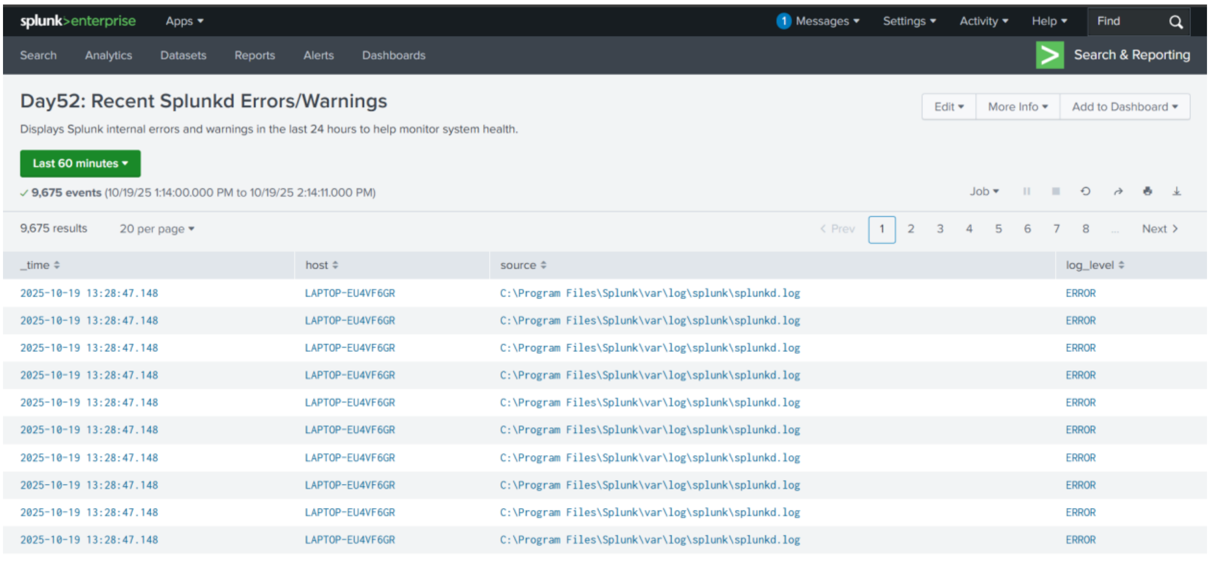
Saved the refined SPL as a reusable report.

- **Command Used:**

  index=_internal sourcetype=splunkd (error OR warn) | table _time host source log_level

- Saved as:
  Day52: Recent Splunkd Errors/Warnings

- Verified under **Reports** section.



Reflection

- **Keyword search felt too broad** during initial queries (index=_internal error) because it matched every log with the word “error.” Using **field filters** (e.g., sourcetype=splunkd) drastically improved relevance.
- **Rule of thumb:** Use table for summaries or structured reporting; stay in **raw view** during early troubleshooting.
- **Most reusable search:**
- index=_internal sourcetype=splunkd (error OR warn)

This query is ideal for **SOC health monitoring** and can be reused for automated alerts.

Summary

This lab demonstrated how to efficiently query and interpret logs using Splunk’s SPL. Skills practiced — Boolean logic, field filtering, wildcards, time range control, and result shaping — are foundational to **SIEM analysis** and real-world **incident response** workflows.