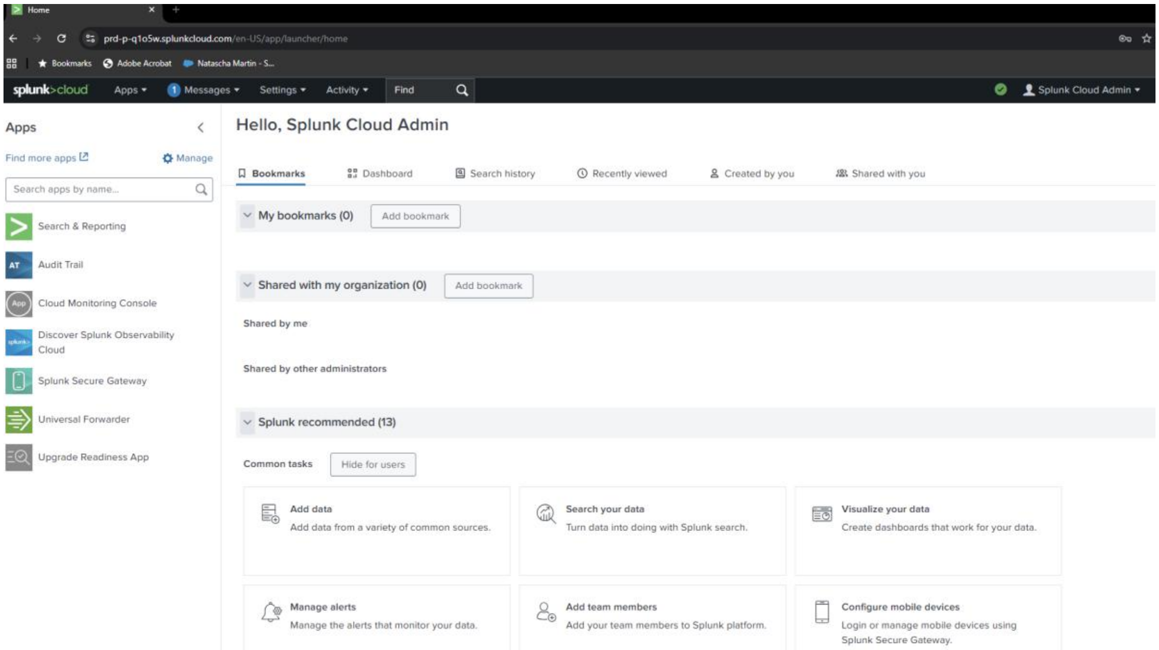
SIEM Tools & Log Analysis Assignment

Overview

This assignment involved using Splunk, a leading Security Information and Event Management (SIEM) tool, to query and analyze log data. The objective was to simulate real-world scenarios where analysts investigate potential threats and trends using log analysis. This included testing Splunk access, querying internal logs, and capturing a real-time system dashboard.

Splunk Cloud Access Verification

Access to a personal Splunk Cloud instance was successfully created. Below is a screenshot of the active session showing the system dashboard and app navigation interface.



Hello, Splunk Cloud Admin

Add data from a variety of common sources.

Turn data into doing with Splunk search.

Create dashboards that work for your data.

Manage the alerts that monitor your data.

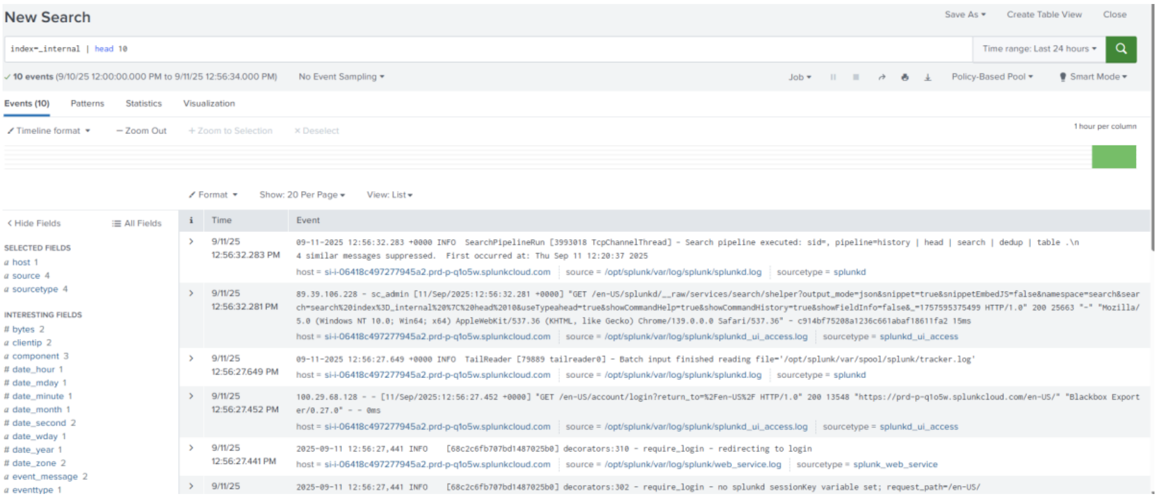
Add your team members to Splunk platform.

Login or manage mobile devices using Splunk Secure Gateway.

Log Query Example

Once inside the Splunk environment, the following test query was prepared to simulate log data retrieval:

```spl
index=_internal | head 10
```



```
index=_internal | head 10
```

✓ 10 events (9/10/25 12:00:00.000 PM to 9/11/25 12:56:34.000 PM)

SELECTED FIELDS
a host 1
a source 4
a sourcetype 4

INTERESTING FIELDS
# bytes 2
a clientip 2
a component 3
# date_hour 1
# date_mday 1
# date_minute 1
a date_month 1
# date_second 2
a date_wday 1
# date_year 1
# date_zone 2
a event_message 2
a eventtype 1

```
i  Time                 Event
>  9/11/25              09-11-2025 12:56:32.283 +0000 INFO  SearchPipelineRun [3993018 TcpChannelThread] - Search pipeline executed: sid=, pipeline=history | head | search | dedup | table .\n
   12:56:32.283 PM      4 similar messages suppressed.  First occurred at: Thu Sep 11 12:20:37 2025
                        host = si-i-06418c497277945a2.prd-p-q1o5w.splunkcloud.com | source = /opt/splunk/var/log/splunk/splunkd.log | sourcetype = splunkd
>  9/11/25              89.39.106.228 - sc_admin [11/Sep/2025:12:56:32.281 +0000] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&sear
   12:56:32.281 PM      ch=search%20index%3D_internal%20%7C%20head%2010&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1757595375499 HTTP/1.0" 200 25663 "-" "Mozilla/
                        5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36" - c914bf75208a1236c661abaf18611fa2 15ms
                        host = si-i-06418c497277945a2.prd-p-q1o5w.splunkcloud.com | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
>  9/11/25              09-11-2025 12:56:27.649 +0000 INFO  TailReader [79889 tailreader0] - Batch input finished reading file='/opt/splunk/var/spool/splunk/tracker.log'
   12:56:27.649 PM      host = si-i-06418c497277945a2.prd-p-q1o5w.splunkcloud.com | source = /opt/splunk/var/log/splunk/splunkd.log | sourcetype = splunkd
>  9/11/25              100.29.68.128 - - [11/Sep/2025:12:56:27.452 +0000] "GET /en-US/account/login?return_to=%2Fen-US%2F HTTP/1.0" 200 13548 "https://prd-p-q1o5w.splunkcloud.com/en-US/" "Blackbox Export
   12:56:27.452 PM      er/0.27.0" - - 0ms
                        host = si-i-06418c497277945a2.prd-p-q1o5w.splunkcloud.com | source = /opt/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access
>  9/11/25              2025-09-11 12:56:27,441 INFO    [68c2c6fb707bd1487025b0] decorators:310 - require_login - redirecting to login
   12:56:27.441 PM      host = si-i-06418c497277945a2.prd-p-q1o5w.splunkcloud.com | source = /opt/splunk/var/log/splunk/web_service.log | sourcetype = splunk_web_service
>  9/11/25              2025-09-11 12:56:27,441 INFO    [68c2c6fb707bd1487025b0] decorators:302 - require_login - no splunkd sessionKey variable set; request_path=/en-US/
```

Observations & Reflections

The instance loaded successfully and displayed the full set of preinstalled apps including Search & Reporting, Cloud Monitoring Console, and Audit Trail. While log querying was not executed in this screenshot, the setup verifies access, dashboard availability, and platform readiness.

Conclusion

This assignment demonstrated the process of accessing and preparing a SIEM platform for log monitoring and analysis. Real-time screenshot evidence validates access. This skill directly applies to cybersecurity roles involving threat detection, compliance auditing, and log correlation.

Summary of Actions Performed

For this assignment, I successfully accessed the Splunk Cloud Platform and performed a basic log query using the Search & Reporting app. I ran the SPL command `index=_internal | head 10` to retrieve the latest internal events generated by Splunk. The results returned HTTP access logs, system activity, and user agent details. I reviewed the log fields, including `source`, `sourcetype`, and `host`, and identified metadata such as time stamps, user activity, and system events. This exercise demonstrated my ability to navigate a SIEM platform, execute queries, and analyze logs to extract relevant security data, a foundational skill in real-world cybersecurity operations.

Because the original Coursera lab environment was locked after course completion, I completed this task manually using a free Splunk Cloud instance to replicate the experience and meet the assignment objectives.