Project Tile: Log Analysis & Threat Detection Using Splunk: Data Ingestion to Dashboarding.

Project Description: This project focuses on ingesting and analyzing login event data using Splunk's Search & Reporting capabilities. Learners will upload a structured dataset, apply SPL queries to identify login success and failure patterns, and build interactive dashboards to visualize. The goal is to develop practical skills in log analysis, data-driven investigation, and dashboard creation within a cybersecurity context.

1. Prepare the Dataset Create or download a structured log file (e.g., sample.csv) containing login events with fields like timestamp, username, IP address, and status (success/failure).

HDFS_2k.log_structured_status.xlsx – excel link

Upload the Data to Splunk Open the Splunk Search & Reporting app → go to Settings → Add Data → Upload → select your file → choose source type (csv) → assign it to an index (e.g., main or bootcamp_logs) → submit.

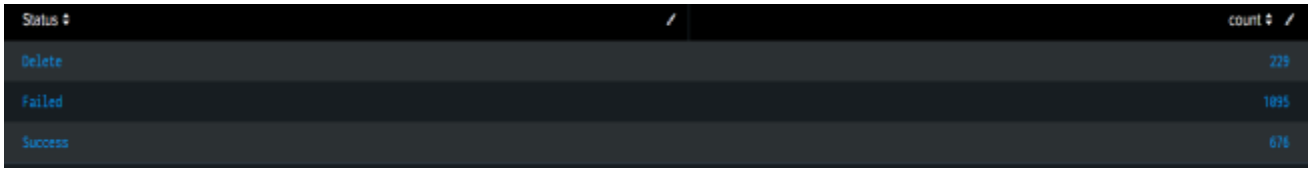
Saved as devtbootcamp_log

. Run SPL Queries to Analyze Login Events Use search queries to count login successes and failures, identify patterns by username or IP, and visualize trends over time.

1. count login successes and failures
   index=devtbootcamp_log| stats count by Status
   query

```
index=devtbootcamp_log | stats count by Status
```

   Output/result



2. identify patterns by username

I have used pid instead of username for quick and easy analysis

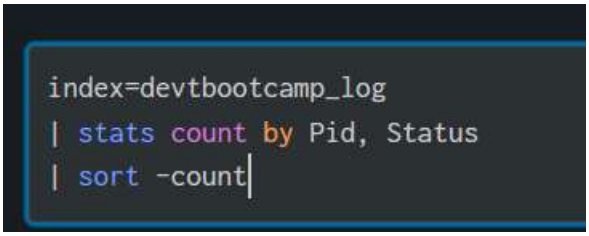
2.identify patterns by username(pid)

index=devtbootcamp_log

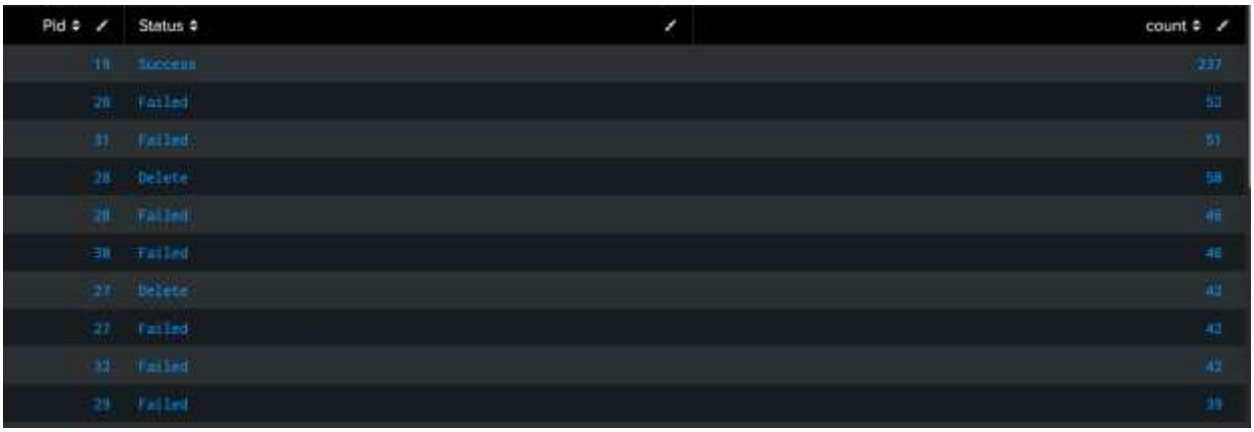
| stats count by Pid, Status

| sort -count

Query



Output/result



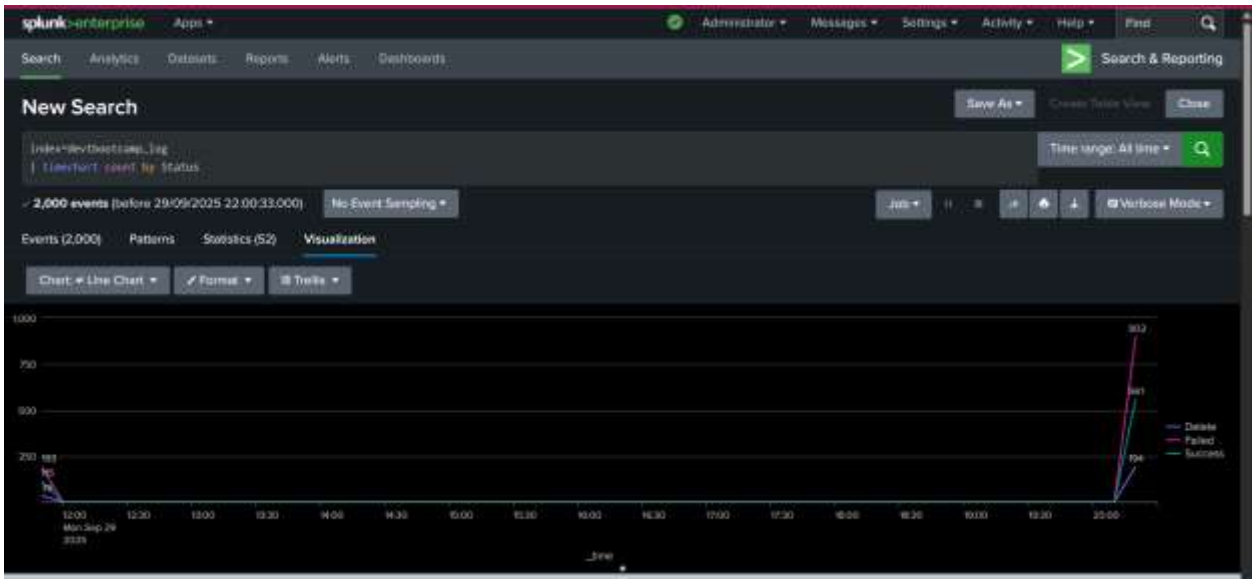
3.visualize trends over time

index=devtbootcamp_log
| timechart count by Status

query

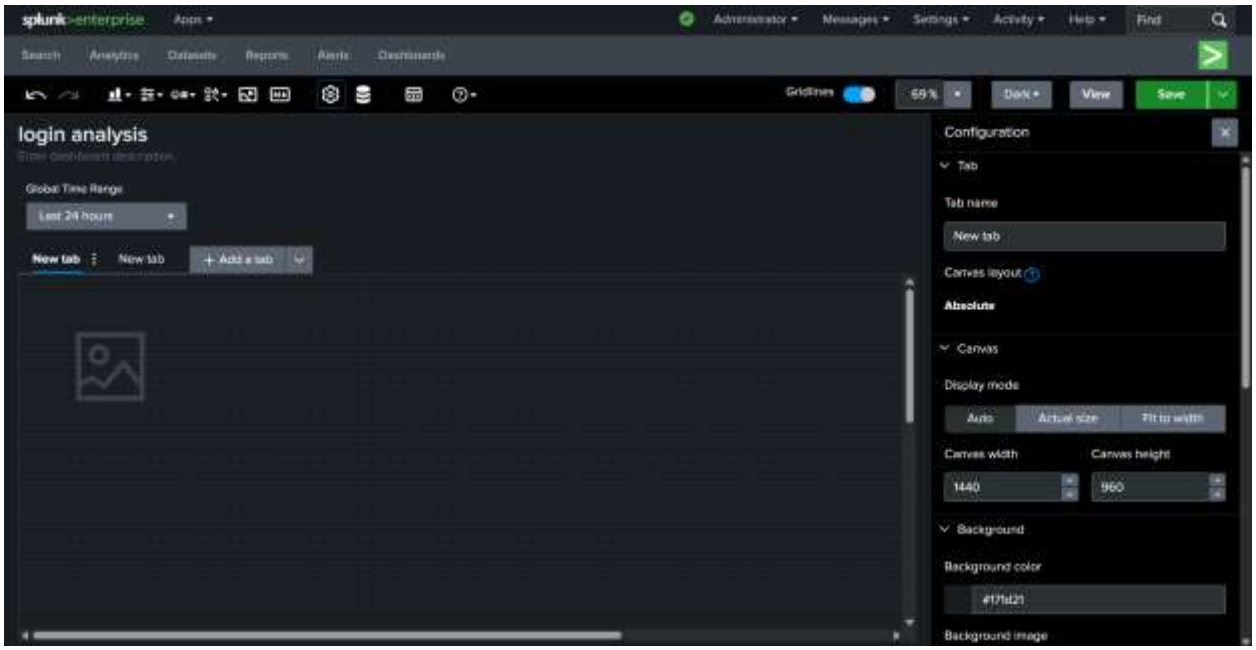
```
index=devtbootcamp_log
| timechart count by Status
```

Output/result
(visualization)

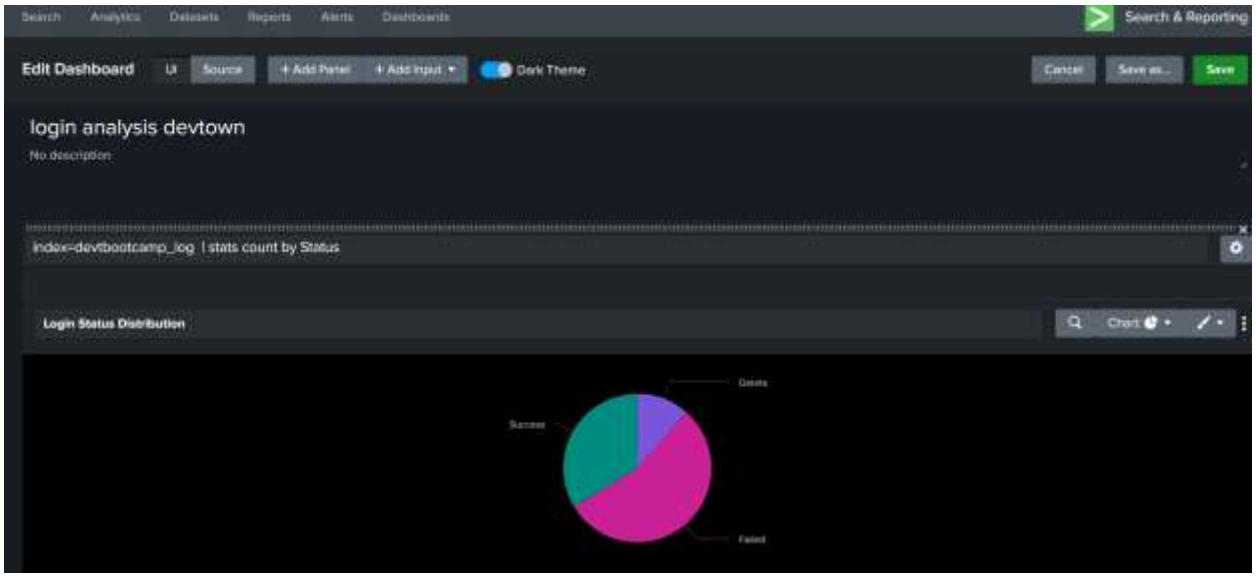


Dashboard: login analysis

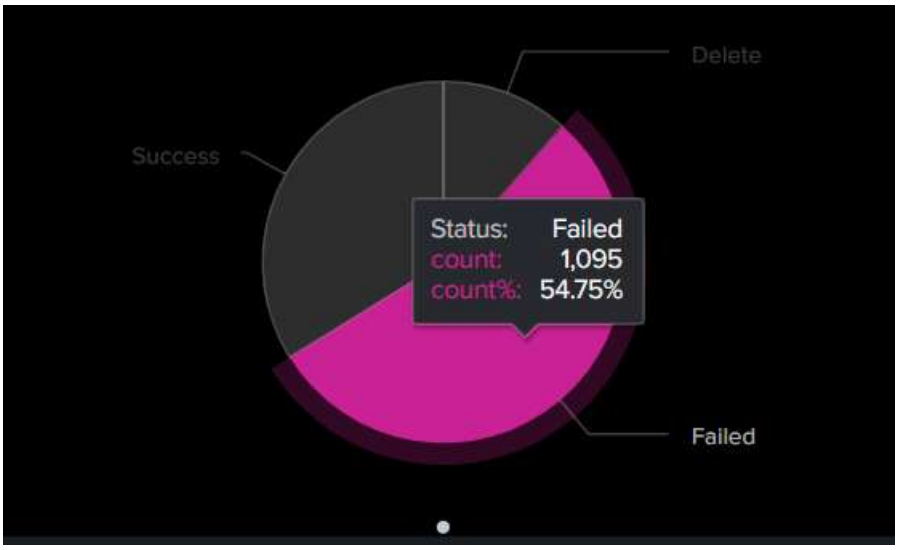
1.Creating a dashboard



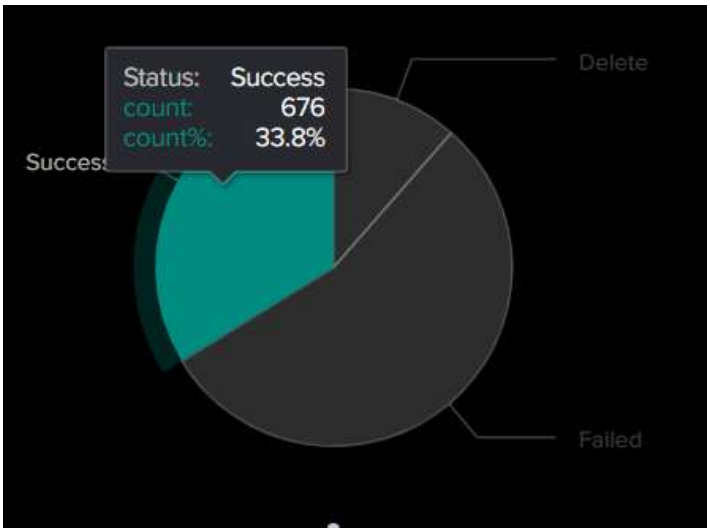
1. index=devtbootcamp_log| stats count by status



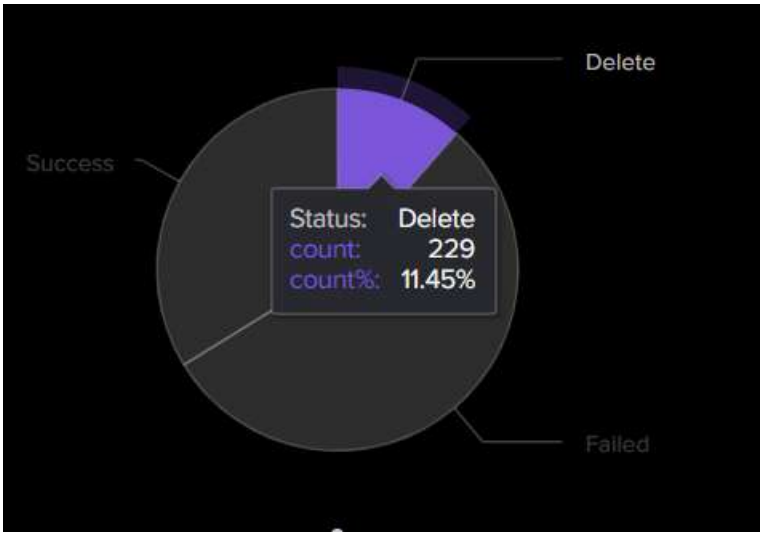
Failed analysis



Passed analysis



delete analysis

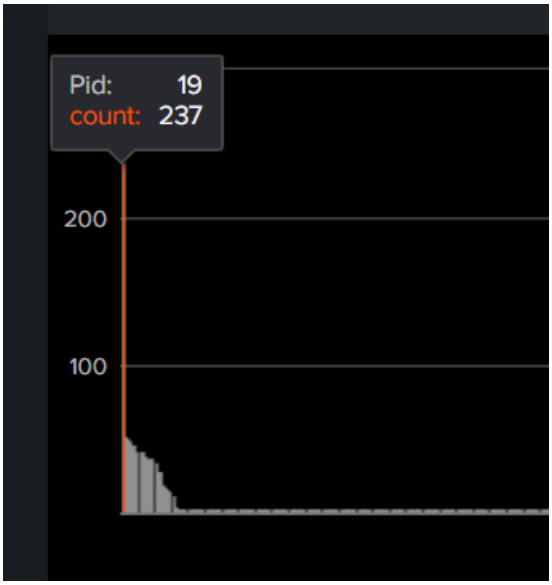


2.identify patterns by username

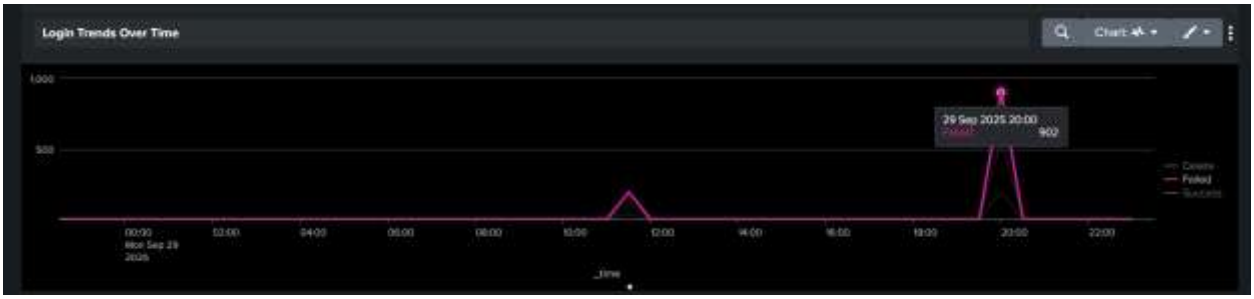
index=devtbootcamp_log status="Failed"

| stats count by pid

| sort -count

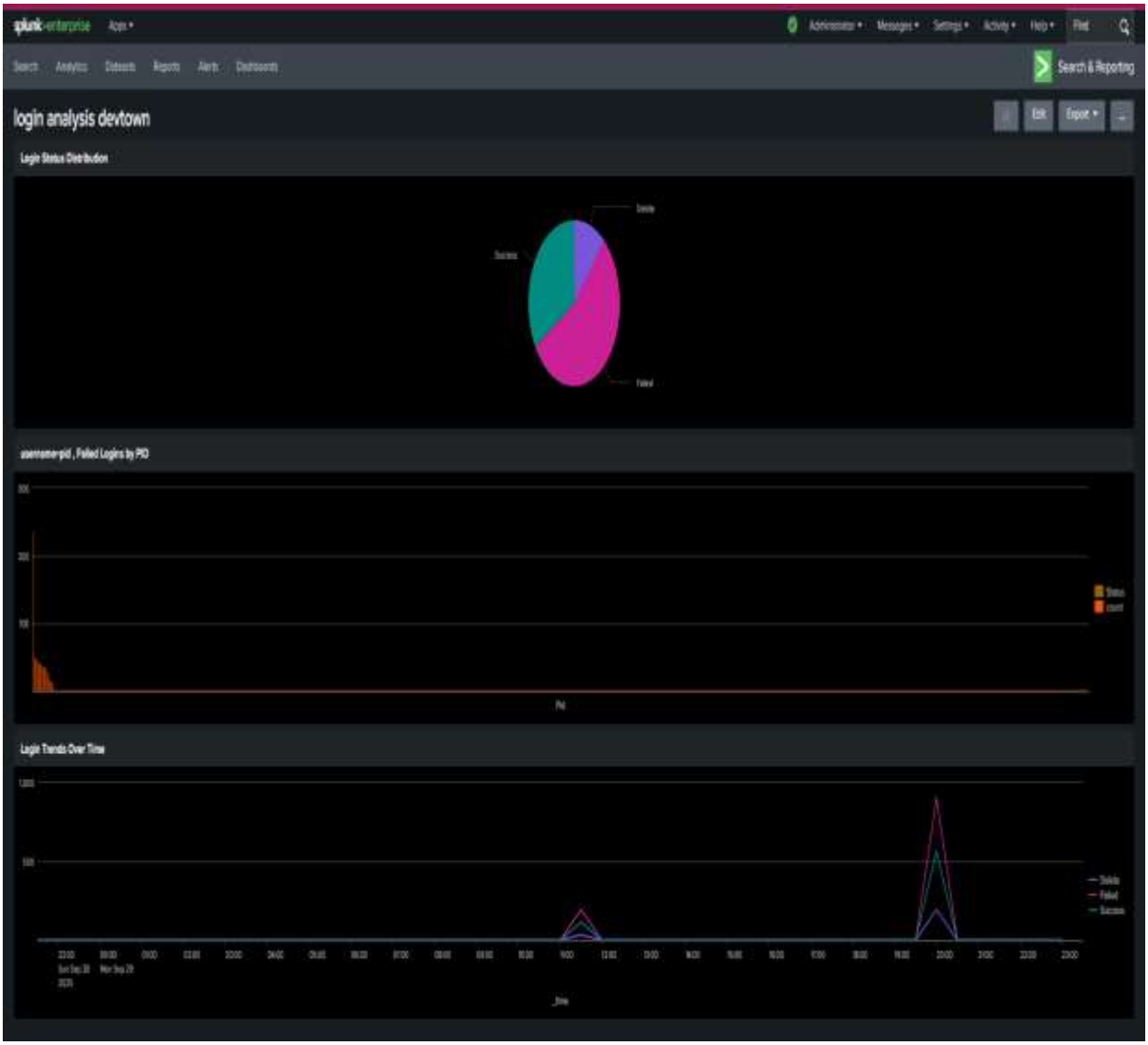


2. visualize trends over time.
   index=devtbootcamp_log
   | timechart count by Status



Overall dashboard in splunk

Link > C:\Users\lakka\Downloads\login_analysis_devtown-2025-09-29.pdf



Analysis

Data arrangement
The data sourced through GitHub https://github.com/logpai/loghub
The status success and failed was missing or interpreted as component
Made a column as status (success, failed, delete) and fixed for ease in analyzing the dataset and inserting the queries

In 1st query
count login successes and failures (index=devtbootcamp_log| stats count by Status)

this query is used to bring out login attempts and address them in categories as (success, failed, delete) determination of bypass or not or anyother reason to enter into the application

these data determine any phishing, or injecting attempts being in run and help the cyber authority for actions

2nd query

2. identify patterns by username

I have used pid instead of username for quick and easy analysis

2.identify patterns by username(pid)

index=devtbootcamp_log

| stats count by Pid, Status

| sort -count

This query determines username particularly taking more attempts to login which concludes the phishing or suspicious behavior compared to other

In this dataset (Pid 19) tool whole lot of attempts for login

3.visulaizing trends

Understanding trend behaviour or _timestamp

Query

```
index=devtbootcamp_log
| timechart count by Status
```

This query is used to analyse login data of customers with respect to time , at what time what attempt is taken to analyze time with respect to login attempt
More failed attempts at night indicate suspicious activity

With all that further same explanation dashboard too are created interative and with informative details

with this I conclude my
Log Analysis & Threat Detection Using Splunk: Data Ingestion to Dashboarding.
Project/assignment

I have learnt to use SPL queries and make visual appealing dashboard by this project
And learnt concepts and practicality from 5 days Splunk bootcamp