Login Anomaly Detection - Splunk App

# Team & Project Info

App Name: Login Anomaly Detection  
Team Name:   
Members: Srinivas , Chaitanya lahari

# 1. Problem Statement

Cybersecurity threats such as brute-force attacks, compromised accounts, and credential abuse are increasingly difficult to detect using traditional rule-based systems. Behavioral anomalies such as logins from unusual geolocations ("impossible travel") or sudden spikes in failure rates often go unnoticed without automated analysis.4

**Objective:** Build a Splunk app that detect anomalous login activity from authentication logs in real-time.

# 2. Solution Overview

This Splunk app uses the Machine Learning Toolkit (MLTK) and KMeans Clustering to identify suspicious login behaviors. It clusters users based on behavioral metrics, flags anomalies, and triggers real-time alerts. It works with CIM-compliant authentication logs and includes dashboards for visualization.

* Key Components:
* Synthetic data ingestion via synthetic\_auth\_logs.csv
* Feature engineering: failure\_ratio, login\_hour, total\_logins, unique\_ip\_count
* KMeans clustering trained to group behavior (Cluster 0 = anomalous)
* Triggers alerts and visualizes risk in dashboards
* Includes Impossible Travel Detection, highlighting logins from distant geolocations within short time gaps

# 3. Machine Learning Approach

Model Type: Unsupervised clustering using Kmeans

Toolkit: Splunk MLTK

Training Data: synthetic\_auth\_logs.csv (CSV with CIM-like fields)

### Features Used:

| Feature | Description |
| --- | --- |
| login\_hour | Hour extracted from timestamp |
| failure\_ratio | Login failure rate per user/hour |
| total\_logins | Total login attempts in the session |
| unique\_ip\_count | Count of distinct IPs per user per hour |

### Model Evaluation:

- Best silhouette score: \_\_\_ at k = 4  
- cluster = 0 identified as anomalous (high failure logins)

# 4. Alerts Implemented

1. Anomalous Login Alert  
- Logins falling in Cluster 0 are flagged and alerted via email as potential brute-force or compromised login behavior.

SPL Query:  
index=main sourcetype="csv"

| eval login\_hour = tonumber(strftime(\_time, "%H"))

| stats count as total\_logins,

sum(eval(action="failure")) as failures

by user, login\_hour

| eval failure\_ratio = failures / total\_logins

| apply login\_anomaly\_kmeans\_model

| where cluster = 0

2. Impossible Travel Alert  
- Flags users who log in from two different countries within 1 minute.

- This flags suspicious activity like simultaneous logins from geographically distant regions.

SPL Query:

index=main sourcetype="csv"

| sort 0 user \_time

| streamstats current=f window=1

last(\_time) as prev\_time,

last(country) as prev\_country

by user

| where isnotnull(prev\_time) AND country != prev\_country

| eval time\_diff\_sec = (\_time - prev\_time)

| eval travel\_type = if(time\_diff\_sec < 3600, "Impossible Travel", "Unlikely Travel")

| eval time\_diff\_human = tostring(time\_diff\_sec, "duration")

| convert ctime(\_time) AS \_time

| convert ctime(prev\_time) AS prev\_time

| table user, \_time, prev\_time, country, prev\_country, time\_diff\_sec, time\_diff\_human, travel\_type

## 5. Dashboard & Visuals

We built a 7-panel interactive dashboard with:

| Panel | Description |
| --- | --- |
| Login Activity Monitor | Area chart of success/failure over time |
| Top Users by Volume | Bar chart of most active users |
| Login Heatmap by Hour | Heatmap: users vs login hours |
| Anomalous vs Normal | Post-scoring result comparison |
| Failure Ratio (Anomalous) | Scatter plot of risky users |
| Anomaly Trend Over Time | Timechart: anomalies by hour |
| Top Risky Users | Table listing high-risk users (cluster 0) |

# 6. Real-World Use Cases

• Account compromise detection  
• Insider threat monitoring  
• Geolocation-based anomaly identification  
• Behavioral security automation

# GitHub Repo & Contacts

- GitHub: https://github.com/srinivas0307/Login-Anomaly-Detection-App  
- Email: srinivasbilluri2005@gmail.com,gurramlahari84@gmail.com

Thank you! This project was built as part of the Splunk Build-a-thon 2025.