

Title: Visualizing Security Event Data Using Power BI

Project Overview:

This project demonstrates how Power BI can be used to analyze and visualize security event data. The report includes details of failed logins, time-based trends, and top source IPs contributing to potential risks. The data insights can help organizations enhance their security posture.

Tools Used:

- **Power BI Desktop**
- **CSV Dataset:** Security Event Logs
- **Data Source:** Sample security logs (failed login attempts, successful logins, source IPs, etc.)

Steps Involved:

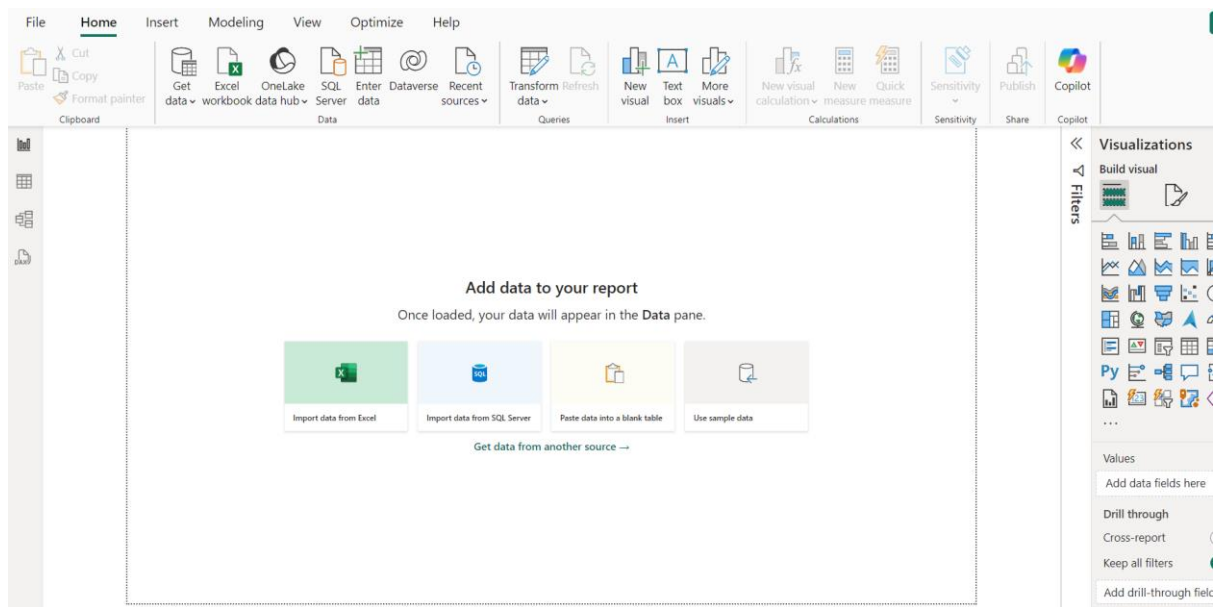
Step 1: Preparing the Dataset

- Used a sample CSV file containing fields like Event ID, Event Type, Source IP, Destination IP, User, Timestamp, and Status.
- Example Dataset:

Event ID	Event Type	Source IP	Destination IP	User	Timestamp	Status
1001	Failed Login	192.168.1.2	192.168.1.100	admin	2025-01-08 14:30:00	Failed
1002	Successful Login	192.168.1.3	192.168.1.101	user1	2025-01-08 14:32:00	Success
1003	Failed Login	192.168.1.4	192.168.1.100	admin	2025-01-08 14:35:00	Failed
1004	Failed Login	192.168.1.5	192.168.1.100	guest	2025-01-08 14:40:00	Failed

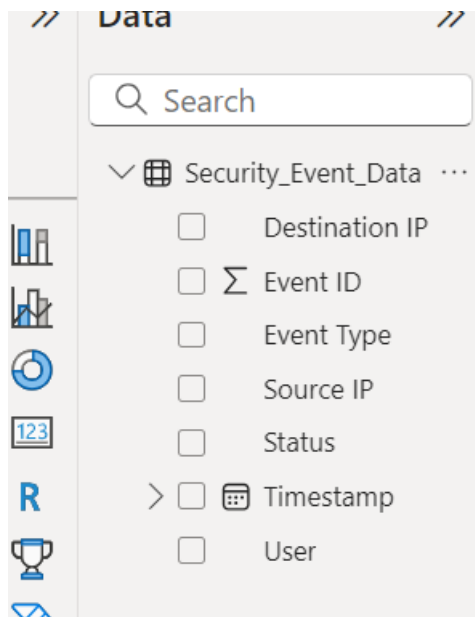
Step 2: Importing Data into Power BI

1. Open Power BI Desktop.
2. Click on **Get Data** and select **CSV**.
3. Import the sample dataset into Power BI.
4. Verify that the data is loaded successfully into Power BI's Data Pane.



Step 3: Data Cleaning and Preparation

- Checked for missing or irrelevant fields.
- Formatted timestamps and ensured event types were categorized properly.



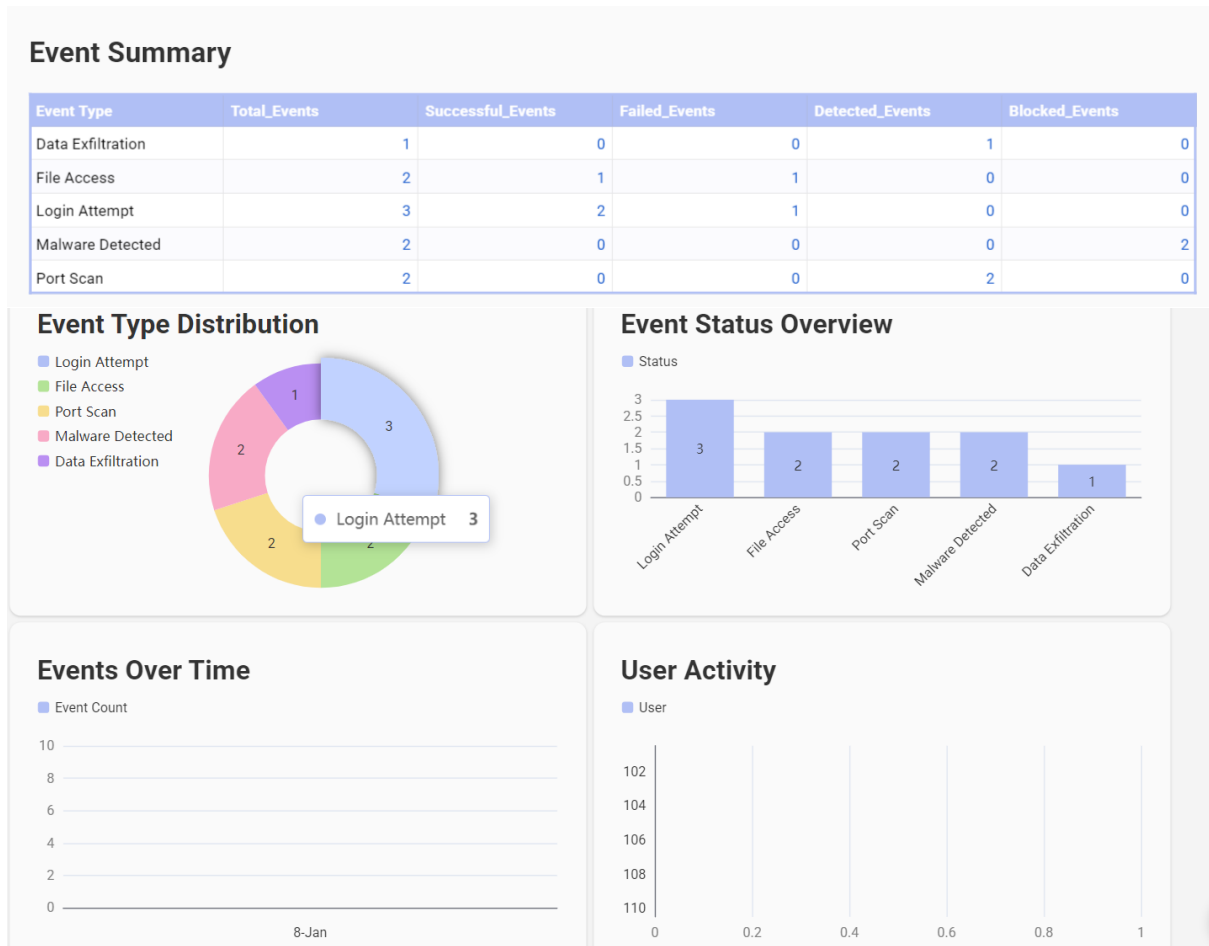
Step 4: Build Visualizations

1. In the **Report View**, drag the following fields to create visuals
 - **Pie Chart:** Show the distribution of Event Type values.

- **Bar Chart:** Display the count of Status (Success, Failed, Detected, Blocked).
- **Table:** Display details such as Event ID, Timestamp, and User

Step 5: Final Dashboard Creation

- Combined all visualizations into a single interactive dashboard.



Conclusion:

This project demonstrates the effective use of Power BI to analyze and visualize security event data. By creating interactive dashboards, organizations can gain actionable insights into their security posture and respond to potential threats proactively.

